Manual do Usuário
AG 30

Outubro 2015, 200.0521.00-7 Rev. 029

Copyright© Digistar, São Leopoldo - RS, Brasil.

Todos os direitos reservados.

A Digistar se reserva o direito de alterar as especificações contidas neste documento sem notificação prévia. Nenhuma parte deste documento pode ser copiada ou reproduzida em qualquer forma sem o consentimento por escrito da Digistar.

TERMO DE GARANTIA:

Para utilizar os serviços de garantia de seu AG 30 Plus Digistar, você precisará apresentar cópia da Nota Fiscal de Compra do produto, com data de emissão legível e enviar para o Centro de Reparos da Digistar (CRD). As despesas com frete serão por conta do cliente.

SUPORTE TÉCNICO:

Ao contatar o Suporte Técnico da Digistar, tenha as seguintes informações disponíveis:

- Modelo do produto;
- Informações sobre a garantia - dados da Nota Fiscal de Compra;
- Uma breve descrição do problema;
- Nome da empresa que instalou o produto.

Método	Descrição
E-mail Suporte	suporte@digistar.com.br
Telefone	(51) 3579-2200
WEB Site	www.digistar.com.br

SUMÁRIO:

1. Conhecendo o seu AG 30 Plus Digistar 8

1.1. Conteúdo da Embalagem 8

1.2. Características Técnicas 9

1.3. Descrição do Hardware 10

1.3.1. Painel traseiro do AG 30 Plus 10
1.3.2. Painel frontal do AG 30 Plus 11

2. Instalação 12

2.1. Equipamentos necessários 12

2.2. Descrição dos Cabos 12

2.2.1. Cabo da Interface Console 12
2.2.2. Cabo da Interface ETH0 / ETH1 13
2.2.3. Cabo da Interface E1 13

2.3. Conectando a alimentação 14

2.4. Processo de Conexão dos Cabos 14

2.4.1. Conectando a interface Console 14
2.4.2. Conectando a interface Ethernet 14
2.4.3. Conectando a Interface E1 em uma Operadora 15
2.4.4. Conectando a Interface E1 em um PABX 15

3. Configuração via browser 16

3.1. Login 17

3.2. VoIP 21

3.2.1. Configuração do SIP 22
3.2.1.1. Habilitar SIP (Configurações Gerais) 22
3.2.1.2. Habilitar Servidores SIP 24
3.2.2. Configurações SIP Integrado 27
3.2.2.1. Configurar Contas SIP 28
3.2.2.2. Configuração de RTP 29

3.3. TDM 30

3.3.1. Tronco Digital 30
3.3.1.1. Status 35
3.3.1.2. Analise de Dígitos (E1 Master) 36
3.3.2. Grupos 37
3.3.2.1. Tom Local 38
3.3.3. Redirecionamento 39
3.3.3.1. Adicionar Regra 39
3.3.3.2. Expressões de Associação 42
3.3.3.3. Expressões de Substituição 43
3.3.3.4. Ordem de execução das regras: 44
3.3.4. Casos de uso 44
3.3.4.1. Caso 1 44

3.3.4.2. Caso 2 46
3.3.5. Status 48
3.4. Manutenção 49
3.4.1. Firmware 49
3.4.2. Versões 49
3.4.3. Upgrade de Firmware 50
3.4.4. Configuração 51
3.4.5. Download 51
3.4.6. Upload 51
3.4.7. Misc 52
3.4.8. Mensagens Binárias 52
3.4.9. Reset Geral 52
4. Configurações de Sistema via CLI 53
4.1. Para acesso via CLI 55
4.1.1. Line VTY 55
4.1.2. Line console 55
4.2. Interface 56
4.2.1. Atraso 57
4.2.2. DHCP 57
4.2.3. Adição de VLANs 59
4.2.4. Q in Q: VLAN sobre VLAN 59
4.2.5. Outras configurações da interface 61
4.2.6. Internet Protocol Version 6 (IPv6) 63
4.2.6.1. Considerações Iniciais 63
4.2.6.2. Configuração de Endereços IPv6 65
4.2.6.3. Configuração Router Advertisements (RA) 69
4.2.7. CPE(config-interface)# ipv6 nd *advertisement-interval* 72
4.2.7.2. Configuração de Servidor DHCP 76
4.2.7.3. Configuração de Relay DHCP 78
4.2.7.4. Configuração de Cliente DHCP sem obtenção de endereço 78
4.3. DNS 79
4.4. DNS Dinâmico 79
4.5. Virtual Router Redundancy Protocol – VRRP 80
4.5.1. Adição de VRRP Track 83
4.6. Bidirectional Forwarding Detection – BFD 84
4.6.1. Configuração do BFD nos protocolos de roteamento 86
4.7. Permissões 86
4.7.1. Access Control Lists - ACLs 86
4.7.1.1. Adição de ACLs 86
4.7.2. Network Address Translation – NAT 91
4.7.2.1. Permitindo o acesso de usuários internos à Internet 91
4.7.2.2. Permitindo o acesso à dispositivos internos a partir da Internet 92
4.7.3. Unicast Reverse Path Forwarding- URPF 93
4.8. Roteamento 94
4.8.1. Adição de Rotas Estáticas 95

4.8.2. Routing Information Protocol – RIP 96
4.8.3. Open Shortest Path First – OSPF 98
4.8.3.1. Configurações específicas de área no OSPF 101
4.8.3.2. Criação de virtual links 102
4.8.3.3. Configuração de parâmetros do OSPF nas interfaces 103
4.8.3.4. Verificação das informações do OSPF 105
4.8.3.5. Configuração de BFD no OSPF 106
4.8.3.6. OPAQUE LSA 106
4.8.4. Open Shortest Path First v3– OSPFv3 108
4.8.4.1. Configurações específicas de área no OSPFv3 110
4.8.4.2. Configuração de parâmetros do OSPFv3 nas interfaces 111
4.8.4.3. Autenticação em links OSPFv3 112
4.8.5. Border Gateway Protocol 113
4.8.5.1. Configurações do BGP 114
4.8.6. Acessa o modo de configuração do roteador BGP. O parâmetro as-number deve ter valores de 1 até 4294967295. 114
4.8.7. Para desabilitar o roteador BGP usa-se: 114
4.8.7.1. Multiprotocol BGP 117
4.8.7.2. RouteReflectors 118
4.8.7.3. Autonomous System Confederations for BGP 119
4.8.7.4. BGP Multipath 120
4.8.7.5. BGP Multihop 120
4.8.7.6. Graceful Restart para BGP 121
4.8.7.7. Filtragem de rotas BGP com access lists 122
4.8.7.8. Filtragem de rotas BGP com prefix-lists 123
4.8.7.9. Uso de route maps no BGP 125
4.8.7.10. BGP Route Servers 130
4.8.7.11. Agregação de rotas no BGP 131
4.8.7.12. Configuração de BFD no BGP 133
4.8.8. IP Multicast 134
4.8.8.1. Modos e Protocolos Suportados 136
4.8.8.2. Configuração de IP Multicast 136
4.8.8.3. Rotas Multicast Manuais 137
4.8.8.4. Protocol Independent Multicast (PIM) 138
4.8.9. Multi Protocol Label Switching 141
4.8.9.1. Configuração 142
4.8.10. VRF-Lite 144
4.8.10.1. Configuração 144
4.8.11. MPLS VPN 145
4.8.11.1. Configuração 145

4.9. Authentication, Authorization e Accounting – AAA 148

4.9.1. Adição de usuários na base de dados do CPE 149
4.9.2. Radius e TACACS+ 150
4.9.2.1. Configurações do RADIUS 151
4.9.2.2. Configurações do TACACS+ 152

4.10. Quality of Service (QoS) 155

4.10.1. Visão Geral dos Mecanismos Suportados 156
4.10.2. Controle de Congestionamento 159
4.10.3. Prevenção de Congestionamento 166
4.10.4. Policiamento e Conformação de Tráfego 168

4.10.5. Table-Map 171
4.10.6. Traffic Policy 174
4.10.6.1. Estatísticas de QoS 190
4.11. Túneis 191
4.12. IP Service Level Agreement (IP SLA) 194
4.12.1. Visão Geral das Operações Suportadas 195
4.12.2. Configuração de IP SLAs 196
4.12.2.1. Configuração de Monitores 197
4.12.2.2. Agendamento de Monitores 213
4.12.3. Visualização de Estado e Configurações 217
4.12.3.1. Estado do IP SLA Monitor 217
4.12.3.2. Configurações do IP SLA Monitor 218
4.12.3.3. Agendamentos do IP SLA Monitor 218
4.12.3.4. Obtenção de Resultados e Estatísticas 219
4.12.4. Reações e Limiares de Operações SLA 220
4.12.4.1. Configuração dos Limiares e Reações 220
4.12.4.2. Gatilho - Reagir com a Ativação de um Outro Monitor 223
4.13. Tracks 224
4.13.1. Tracking de Rotas IP 224
4.13.1.1. Se é Alcançável 225
4.13.1.2. Usando Limiares de Métrica 225
4.13.2. Tracking de Operações SLA 226
4.13.2.1. Se a Operação Alcança o Destino 227
4.13.2.2. Pelo Estado do SLA-Threshold 228
4.13.3. Tracking de Interfaces 229
4.13.3.1. Protocolo de Linha 229
4.13.3.2. Roteamento IP 230
4.14. Internet Protocol Security (IPsec) 231
4.14.1. Considerações Iniciais 231
4.14.2. Mecanismos Suportados 233
4.14.3. Cenários de Uso 234
4.14.3.1. Host-to-Host 234
4.14.3.2. Net-to-Net 234
4.14.3.3. VPN 235
4.14.4. Configuração 235
4.14.4.1. Configurações Básicas 236
4.14.4.2. HOST-to-HOST 240
4.14.4.3. NET-to-NET 240
4.14.4.4. VPN/Roadwarrior 241
4.14.5. Exemplos de Configuração usando PSK 242
4.14.5.1. HOST-to-HOST 242
4.14.5.2. NET-to-NET 243
4.14.5.3. VPN 244
4.14.6. Chaves RSA 245
4.14.6.1. Gerando Novas Chaves 246
4.14.6.2. Exportando Chaves 246
4.14.6.3. Importando Chaves 247
4.14.6.4. Excluindo Chaves 247
4.14.7. Certificados X.509 247

4.14.7.1. Configurando Trustpoints 248
4.14.7.2. Obtenção de Certificado Offline 249
4.14.7.3. Obtenção de Certificado Online (SCEP) 251
4.14.7.4. Importando Certificados 251
4.14.7.5. Exportando Certificados 252
4.14.7.6. Configurações Extras 252
4.14.8. Exemplos de Configuração usando Certificados 253
4.14.8.1. Interoperabilidade CISCO (Certificados) 253

4.15. PKI Server 255
4.15.1. Criando um Offline PKI Server 255
4.15.2. Exportando o Certificado desta CA 256
4.15.3. Coletando uma Requisição 256
4.15.4. Autorizando uma Requisição 256
4.15.5. Excluindo todas as Requisições 257
4.15.6. Excluindo uma Requisição 257
4.15.7. Revogando um Certificado 257
4.15.7.1. Revalidando um Certificado Revogado 257

4.16. Conection Fault Management (IEEE802.1ag) 258
4.16.1. Considerações Iniciais 258
4.16.1.1. Configuração 258
4.16.1.2. Habilitando o CFM 258
4.16.1.3. Configurando um Domínio 259
4.16.1.4. Configurando um MEP 261
4.16.1.5. Configurando Alarmes 263
4.16.2. Estatísticas 265
4.16.2.1. Defeitos 265
4.16.2.2. MEPs Locais e Remotos 265
4.16.2.3. Estatísticas de Pacotes CFM 266

4.17. Ethernet Local Management Interface (E-LMI) 267
4.17.1. Considerações Iniciais 267
4.17.2. Configuração de E-LMI 267
4.17.2.1. Configuração Global 268
4.17.2.2. Configuração na Interface 268
4.17.3. Mostra de Estatísticas e Configurações 270

4.18. Serviços 272
4.18.1. HTTP 272
4.18.2. SSH 273
4.18.3. TELNET 274
4.18.4. Simple Network Management Protocol – SNMP 274
4.18.5. Syslog 278
4.18.6. Monitor de fluxo 280
4.18.7. RMON (Remote Monitoring) 282

4.19. Configurações do SIP 285

4.20. Configurações TDM 289

5. Anexo I - Status enviado do SIP para o ISDN no encerramento de ligações. 293

1. Conhecendo o seu AG 30 Plus Digistar

O AG 30 Plus é um gateway que converte tecnologias:

- Converte a tecnologia IP em digital, permitindo que uma rede IP (VoIP) faça a interface de voz, via E1, com a rede PSTN, agregando pontos de presença em diversas localidades e com o custo de uma chamada local.

- Converte a tecnologia digital de um PABX TDM (E1) em IP, permitindo o uso da tecnologia VoIP, sem alterar o PABX existente.

Além disso, o AG 30 Plus opera como router de dados para a sua rede de computadores, provendo com um único link IP a solução para dados e voz.

Ao longo deste manual o AG 30 Plus poderá será demoninado de "CPE".

1.1. Conteúdo da Embalagem

- 1 AG 30 Plus
- 1 Manual de instalação
- 1 Fonte de alimentação

1.2. Características Técnicas

Tabela 1: Características Técnicas

Codecs de Áudio: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps)	**Codecs para Fax:** G.711A (64kbps), G.711U (64kbps) e T.38
DTMF: dentro ou fora da banda	**Contas SIP:** até 1.000 contas **Contas SIP Integrado:** 64 contas
Linhas Digitais: capacidade máxima de 30	**Impedância (Porta Digital):** 100 ohms
Sinalização Digital R2/MFC: • De linha: R2 digital ou R2 analógico (E M contínuo) • De registradores: entrada e saída MFC	**E1 (R2 e ISDN):** Master/Slave (Clock Regenerado)
Proteção de Programação: Memória não volátil FLASH	**Alimentação AC:** Entrada full-range: 95 Vac à 240 Vac
Processador: Power Quicc de 32 Bits com 64MB RAM e 32MB de Flash	**Consumo Máximo:** 25 VA
Temperatura de Operação: 10ºC a 40ºC	**Umidade Relativa do Ar:** 20% a 90%
Falta de Energia: Deve ser adicionado No-break	**Instalação:** Mesa, Parede e [1]Rack 19" [1]*Opcional*
Dimensões (mm): A: 40 / L: 220 /P: 130	**Peso Máximo:** 0,9 Kg
Bilhetagem: Via FTP	

1.3. Descrição do Hardware

1.3.1. Painel traseiro do AG 30 Plus

Figura 1: Vista Painel Traseiro

Tabela 2: Descrição dos conectores do AG 30 Plus

Item	Descrição
PWR	Conector para entrada de alimentação (5 VDC)
WAN/ETH1	Conector Superior RJ-45
LAN/ETH0	Conector Inferior RJ-45
E1/T1	Conector E1/T1 RJ-45
CONSOLE	Entrada para console USB

1.3.2. Painel frontal do AG 30 Plus

Figura 2: Vista Painel Frontal

Tabela 3: Descrição dos LED's do AG 30 Plus Digistar

LED	Descrição
PWR	Ligado: quando a fonte do AG 30 Plus está funcionando.
VOIP	Piscando indica ligação VoIP ativa
ETH0/LAN	Desligado indica "link up" em 10Mbps. Ligado indica "link up" em 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "link up"
ETH1/WAN	Desligado indica "link up" em 10Mbps. Ligado indica "link up" em 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "link up"
E1	Link E1

2. Instalação

2.1. Equipamentos necessários

Cabos:
Cabo Console USB-B(F) - USB-A(F) - não incluído
Cabo RJ 45 para LAN / WAN - incluído opcionalmente
Cabo RJ 48 para E1 - incluído opcionalmente

Equipamentos:
PC com entrada USB para terminal de configuração (console)
Navegador WEB (HTTP/HTTPS)
Cliente Telnet ou SSH (CLI)

2.2. Descrição dos Cabos

2.2.1. Cabo da Interface Console

O cabo da porta console possui em uma extremidade um conector USB-B(F) que deve ser conectado no equipamento. A extremidade que deve ser conectada a um computador possui conector USB-A(F).

2.2.2. Cabo da Interface ETH0 / ETH1

O cabo da interface ETH0 / ETH1 é o cabo padrão reto para as interfaces FastEthernet. A interface pode operar tanto em 10Mbps ou 100Mbps, Full-Duplex ou Half-Duplex. Pode ser usado um cabo cruzado, no entanto este não é necessário, pois a interface possui a funcionalidade A*uto Crossover MDI/MDI-X*.

A disposição dos sinais está descrito na tabela abaixo.

Tabela 4: Disposição dos sinais FastEthernet no conector RJ-45

RJ-45	Sinal	Descrição do Sinal
1	TX+	Data Out Circuit +
2	TX-	Data Out Circuit -
3	RX+	Data In Circuit +
4	---	---
5	---	---
6	RX-	Data In Circuit -
7	---	---
8	---	---

2.2.3. Cabo da Interface E1

O cabo para conexão com interface E1 é um cabo padrão RJ 48. A disposição dos sinais está descrito na tabela abaixo:

Tabela 5: Disposição dos sinais FastEthernet no conector RJ-48

RJ-48 (1)	Sinal (1)	RJ-48 (2)	Sinal (2)
1	RX	4	TX
2	RX	5	TX
3	GND	3	GND
4	TX	1	RX
5	TX	2	RX
6	GND	6	GND
7	GND	7	GND
8	GND	8	GND

2.3. Conectando a alimentação

Conecte a fonte de alimentação de acordo com os seguintes passos:

- Passo 1: Conecte extremidade apropriada do cabo de alimentação na entrada DC no painel traseiro do AG 30 Plus e a outra extremidade na tomada 110/220V, 50/60Hz da alimentação.

- Passo 2: Verifique se o LED de alimentação (PWR) do painel frontal do AG 30 Plus está aceso. Caso contrário repita o passo 1.

Se o LED indicador de alimentação permanecer desligado mesmo depois de repetidos os passos 1 e 2 contate o fornecedor.

2.4. Processo de Conexão dos Cabos

2.4.1. Conectando a interface Console

Para configurar o AG 30 Plus através do terminal:

- Passo 1: Prepare um PC de configuração. Se a configuração for remota, dois modems também serão necessários.

- Passo 2: Confirme se o AG 30 Plus e o PC estão desligados e então conecte o PC na porta console do AG 30 Plus via o cabo console USB.

Observação: Requer instalação de Drivers (Windows).
www.digistar.com.br/ag30plus/drivers_usb.zip

2.4.2. Conectando a interface Ethernet

Em um PC ou em um Modem:

- Passo 1: Insira uma extremidade do cabo ethernet na interface Ethernet 10BASE-T/100BASE-TX do AG 30 Plus.

- Passo 2: Insira a outra extremidade do cabo ethernet na interface 10BASE-T/100BASE-TX do PC ou Modem.

- Passo 3: Verifique o LED indicador de estado no painel frontal do AG 30 Plus e o LED da placa de rede do PC e/ou do o LED do Modem.

2.4.3. Conectando a Interface E1 em uma Operadora

Modo Slave:

- Passo 1: Configure a interface do AG 30 Plus como Slave.
- Passo 2: Insira a extremidade da linha E1 fornecida pela operadora na interface E1 do AG 30 Plus.
- Passo 3: Se a interface estiver configurada, aguarde em torno de 1 minuto para estabelecer a conexão dos canais.
- Passo 3: Verifique o LEDs indicadores dos canais no painel frontal do AG 30 Plus.

2.4.4. Conectando a Interface E1 em um PABX

Modo Master:

- Passo 1: Configure a interface do AG 30 Plus como Master.
- Passo 2: Insira a extremidade da linha E1 fornecida pelo PABX na interface E1 do AG 30 Plus.
- Passo 3: Se a interface estiver configurada, aguarde em torno de 1 minuto para estabelecer a conexão dos canais.
- Passo 4: Verifique o LEDs indicadores dos canais no painel frontal do AG 30 Plus.

3. Configuração via browser

Para perfeita funcionalidade, é recomendado sempre utilizar a versão mais recente do Browser.

Versão mínima para configurador WEB:

- Internet Explorer 8
- Firefox 15
- Safari 5
- Chrome 18
- Opera 11

Inicialmente para acessar o Configurador Web , devemos conectar a interface de rede de um PC na interface ethernet 0 do AG 30 Plus. Para tanto, utilize um cabo de rede.Com a conexão correta, devemos configurar o PC para acessar a página. O PC deve ser configurado com gateway 192.168.10.1 e um IP nesta rede.

Após isto, acessaremos o Configurador Web. Para tanto, utilizamos a URL abaixo:

http://192.168.10.1

Observação:
As configurações feitas através de configurador WEB devem ser aplicadas para que tenham validade. Todas as páginas de configuração possuem um botão “Aplica”, e as alterações realizadas em cada página só serão validadas após o click neste botão. As alterações são gravadas em memória volátil tipo RAM, para que elas tenham efeito, gravar as configurações no campo “gravar” localizado na parte superior das páginas.

3.1. Login

Ao acessar a página, aparece a tela de logon, conforme abaixo:

Nesta página o usuário “admin” e usuários autorizados podem optar pela configuração rápida ou configuração normal. Ao escolher a configuração rápida o usuário tem acesso somente às opções mais críticas para o funcionamento do AG 30 Plus. Esse modo foi criado para a primeira customização de uma máquina nova.

Atenção: Ao se encerrar o configurador rápido, todas as configurações atuais serão perdidas!

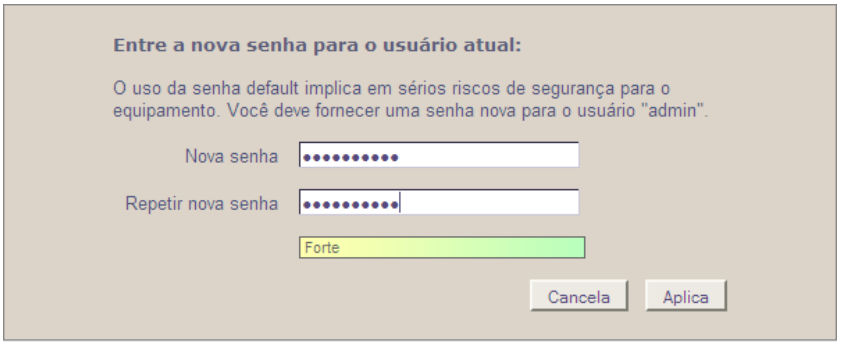
Para acessar, o usuário deve fornecer usuário e senha.

Usuário default: admin e senha default: admin

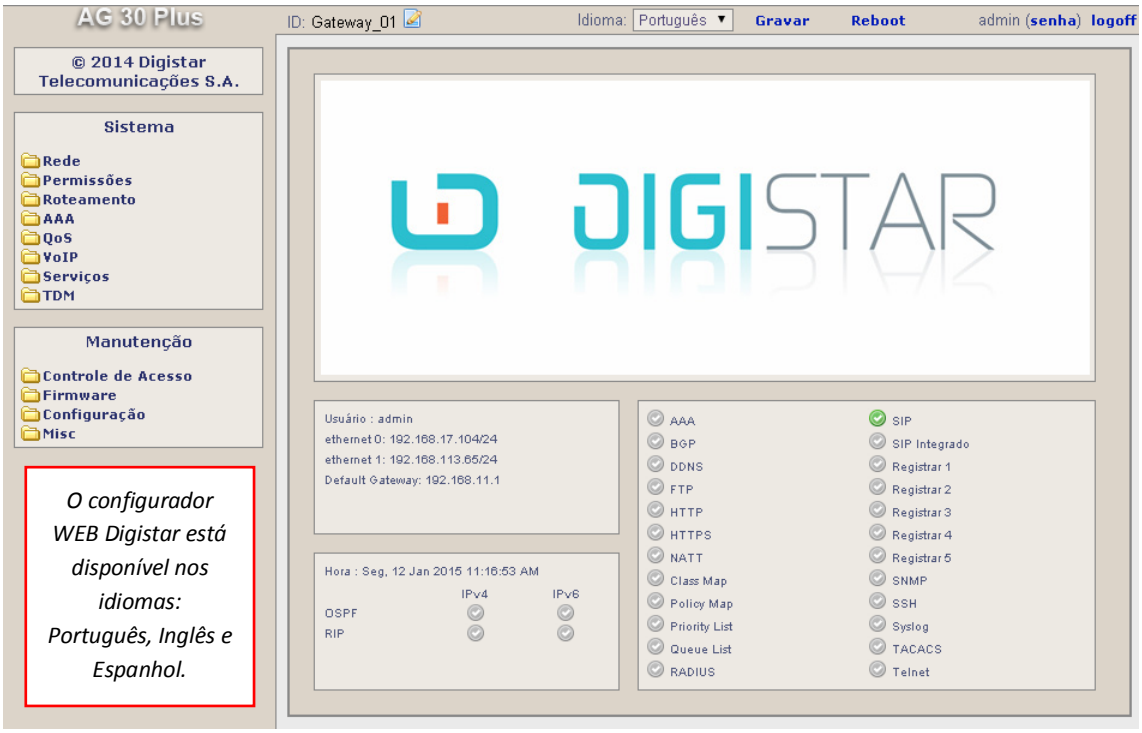
Usuário: até 20 caracteres

Senha: até 16 caracteres

OBS.: *No primeiro acesso do usuário admin com senha default, será requisitada a troca da senha deste usuário. O programa irá validar a senha entrada e indicará sua força com uma barra de progresso. O Botão Aplica só estará habilitado com uma senha forte.*


Entre a nova senha para o usuário atual:
O uso da senha default implica em sérios riscos de segurança para o equipamento. Você deve fornecer uma senha nova para o usuário "admin".
Nova senha
Repetir nova senha
Forte
Cancela
Aplica

Após acessar o configurador com o usuário admin, aparece a tela abaixo:

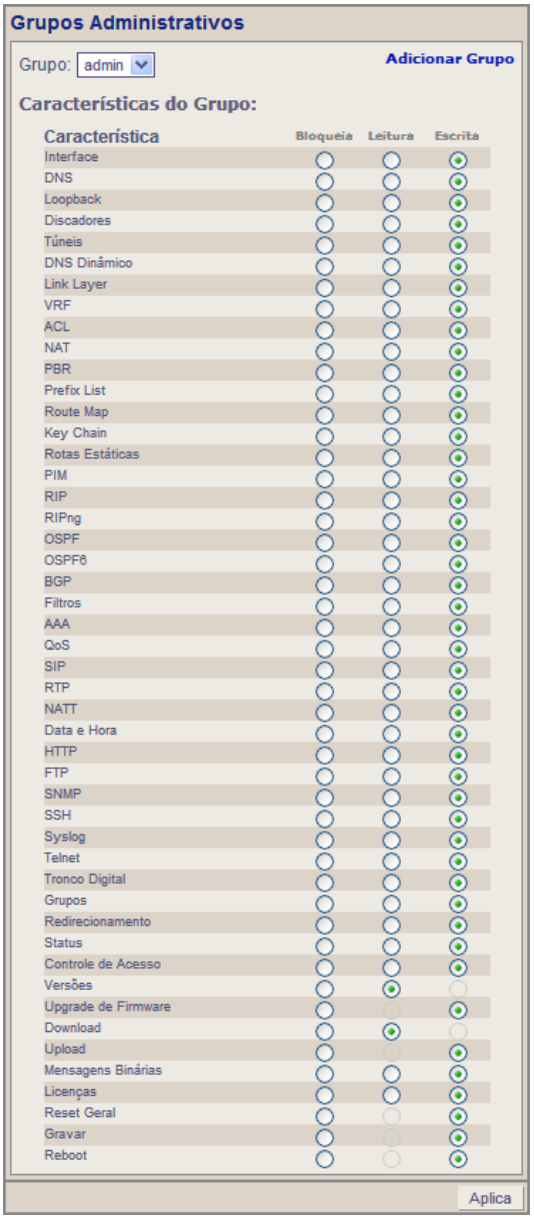


Nesta tela estão localizados um menu a esquerda e uma janela, que exibe algumas configurações de serviços configurados no AG 30 Plus. Estas configurações podem ser acessadas clicando-se sobre os “títulos” ou acessadas através do menu que se encontra no lado esquerdo da tela.

ID: Pode-se associar uma string arbitrária de identificação para o gateway. Essa string, se configurada, aparece na tela de login.

Cadastro Grupos de Usuários (Editar Grupos)

Com o usuário admin é possível cadastrar novos grupos de usuários (em Editar Grupos) e configurar os acessos de cada grupo.



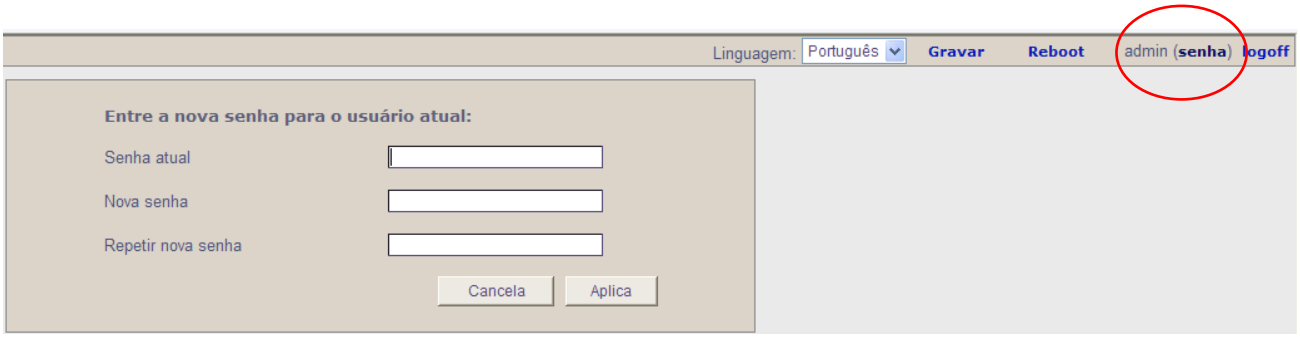
Ao clicar em cima das palavras “Bloqueia”, “Leitura” ou “Escrita” habilita todos os itens.

Cadastro de Usuários (Editar Usuários)

Em “Editar Usuários” podem ser cadastrados os usuários com suas senhas. Cada usuário deve ser associado a um grupo de usuários, pois é lá que são definidas suas permissões.

Alteração da senha

Cada usuário, após logado, poderá alterar sua senha, clicando em “senha” que aparece no canto superior direito, conforme tela abaixo.



OBS.:

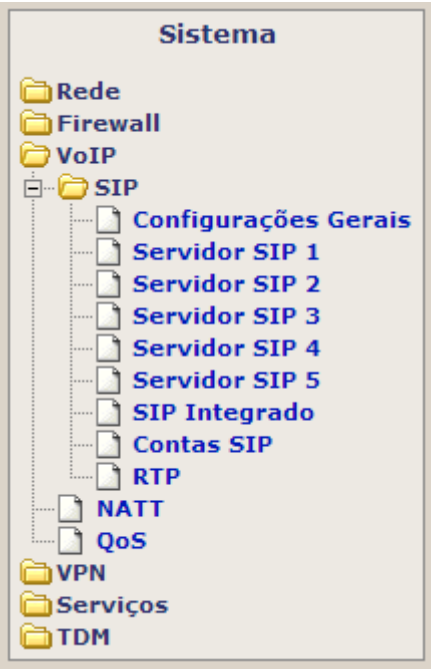
O tempo de inatividade do usuário admin é de 5min.

O tempo de inatividade dos demais usuários pode ser configurado. Os tempos disponíveis são: 1 min, 5 min, 10 min ou 15 min.

É permitido o cadastro de 8 grupos de usuários e 16 usuários.

Não é permitido alterar os acessos do Grupo Admin.

3.2. VoIP



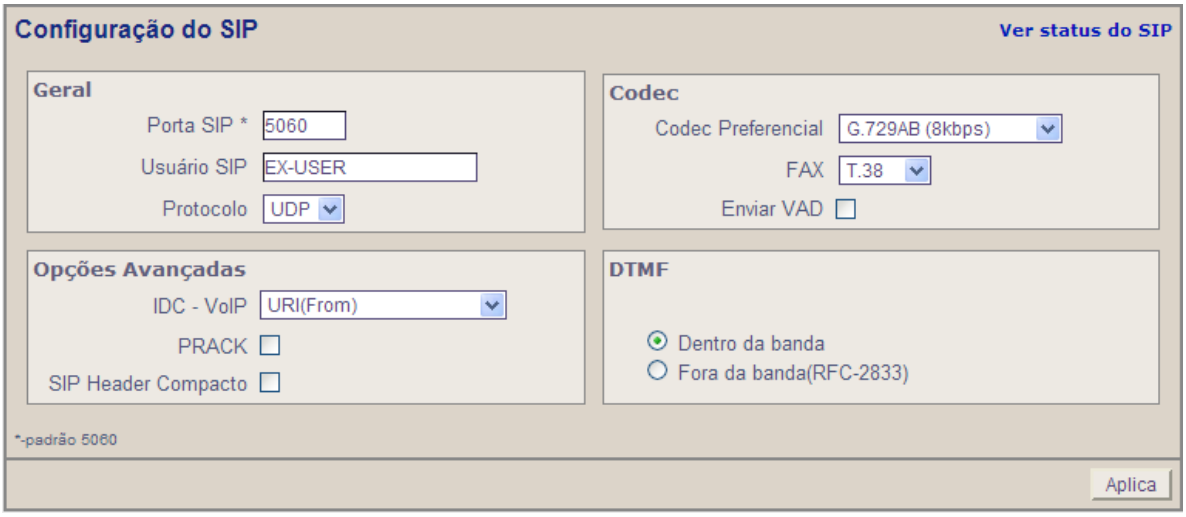
As ligações IP são feitas no VoIP usando o protocolo SIP (Session Initiation Protocol, RFC3261). Este serve para negociar os parâmetros da comunicação via rede, escolhendo endereço e compactação para o envio e recepção de áudio. Depois de estabelecida a chamada, os pacotes de áudio trafegam usando o protocolo RTP (Real-time Transport Protocol, RFC3550 e RFC3551).

O protocolo SIP oferece a opção de usar um servidor SIP (Registrar/Proxy), que funciona como uma central de endereços SIP, onde cada ponto tem um nome de usuário associado ao seu endereço real. Nesse caso todas as mensagens SIP para outros pontos registrados no servidor Registrar/Proxy serão encaminhadas para o servidor, que através de seu banco de dados de usuários registrados irá encaminhá-las para o endereço correto. Isso é usado pelas operadoras VoIP.

Quando uma chamada é negociada, o protocolo de sinalização usado (SIP) precisa passar para o outro ponto de comunicação o endereço para onde deve ser enviado o áudio. Esse endereço precisa ser acessível a partir do outro ponto de comunicação, caso contrário a conexão não terá áudio. Se a WAN do AG 30 estiver conectada à Internet através de um NAPT, ou seja, tiver um endereço IP de uma rede interna não-roteável, o STUN deverá ser habilitado para que as ligações VoIP tenham áudio.

3.2.1. Configuração do SIP

3.2.1.1. Habilitar SIP (Configurações Gerais)



- **Habilitar SIP: Habilita/Desabilita o protocolo SIP para chamadas VoIP.**

Geral:

- Porta SIP: porta local onde serão recebidas as mensagens pertencentes ao protocolo SIP. A porta padrão é 5060.
- Usuário SIP: identificação enviada pelo AG 30 nos pacotes SIP em ligações que não usem o cliente registrar, por exemplo, uma ligação para um número. IP.
- Protocolo: Protocolo de transporte utilizado para sinalização SIP. Os protocolos disponíveis são UDP e TCP. O mais usado é o UDP.

Codec:

- Codec Preferencial: compressão de áudio que terá preferência na negociação da chamada. Caso a outra ponta da chamada não suporte a codificação escolhida, outro codec será usado automaticamente.
- Codecs disponíveis: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps).
- Enviar VAD: Não envia pacotes ou envia pacotes menores quando detecta silêncio.
- FAX: Escolha do codec que será usado para a recepção de FAX via VoIP. Para que o T.38 funcione, o aparelho de FAX que irá receber deve estar configurado para recepção automática. Ao enviar um FAX via VoIP é o ponto que recebe o FAX que determina o protocolo a ser usado.
  Codecs disponíveis: G.711 e T.38.

OBS.: *A funcionalidade T38 poderá não operar corretamente, pois depende das características de rede, tais como: jitter e atraso de rede, bem como da velocidade dos aparelhos de fax envolvidos na conexão.*

- **DTMF:** Método de transmissão de dígitos DTMF, pode ser dentro ou fora da banda. Quando estiver selecionado dentro da banda o DTMF é enviado com o áudio, podendo apresentar distorções que impossibilitam sua detecção pelo equipamento que irá recebê-lo.
  No DTMF fora da banda é usada a norma RFC2833, onde o dígito é enviado em um pacote RTP.

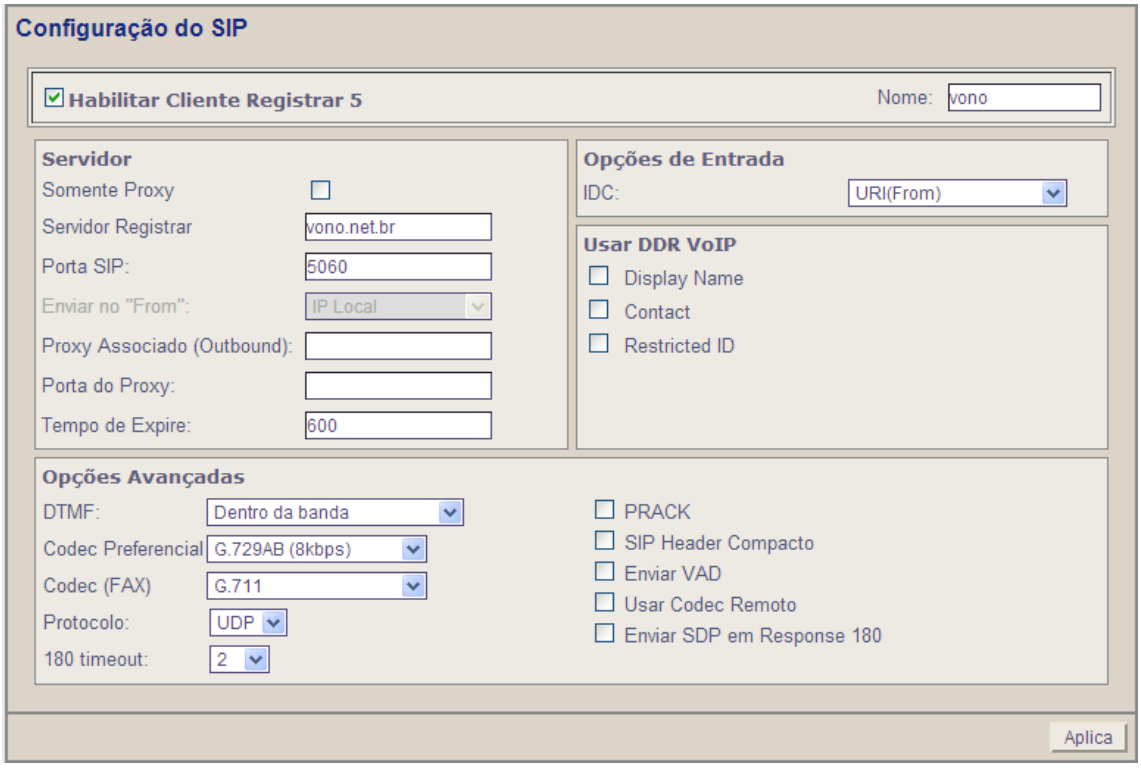
- **Opções Avançadas:**
  - **IDC – VoIP:** Permite configurar qual campo do pacote SIP será utilizado para identificar a origem de ligações de entrada. São disponíveis os campos URI (From), que é o caso mais comum, DISPLAYNAME (From), que permite uma identificação mais amigável, porém é um campo não obrigatório, e URI (Contact), que comumente identifica o dispositivo de origem da ligação.

  - **SIP Header Compacto**: Envia as mensagens SIP com headers compactos (RFC 3261 e RFC 6262).

  - **PRACK:** Habilita a RFC 3262 (Reliable Provisional Responses).

3.2.1.2. Habilitar Servidores SIP

Configuração dos servidores SIP (Registrar/Proxy) que serão utilizados para realizar e receber as ligações VoIP. É possível configurar até cinco (5) servidores SIP.



OBS.: *"É recomendável que o valor configurado no campo "Tempo de Expire" seja inferior a 180 quando o equipamento estiver atravessando um NAT ao se comunicar com o servidor Registrar, para evitar a perda das associações de NAT feitas nos roteadores ao longo da rede entre o equipamento e o servidor. Estas associações de NAT não são permanentes, sendo mantidas enquanto existe comunicação entre os pontos com um timeout típico de 3 minutos"*

- **Habilitar Servidor SIP:** Habilita/Desabilita a utilização do servidor VoIP configurado.

  - ***Nome:*** Identificação amigável da operadora. Este campo pode conter qualquer valor e não é utilizado para a realização das chamadas.

- ***Somente Proxy:*** Esta opção desabilita o envio do pedido de registro para o servidor SIP. As chamadas são encaminhadas para o endereço do servidor SIP Registar/Proxy sem que a mensagem REGISTER seja enviada.

    - ***Enviar no From*****:** indica qual IP será usado na identificação do AG 30 quando este originar uma chamada ao Servidor Proxy, sendo as opções disponíveis: o IP Local do AG 30 ou o IP do Proxy. Para efetuar essa configuração a operadora deve ser consultada quanto à identificação da origem das chamadas.

- ***Servidor Registrar/Proxy:*** endereço IP do servidor Registrar/Proxy.
- ***Porta SIP:*** porta do servidor para a qual serão direcionadas as mensagens do protocolo SIP enviadas pelo AG 30. A porta padrão é 5060.
- ***Tempo de Expire*****:** duração dos registros em segundos. Após esse tempo, caso não tenha sido renovados, os registros são apagados do servidor.
- ***Proxy Associado (Outbound):*** endereço do servidor que irá redirecionar os pacotes para o servidor Registrar/Proxy.
- ***Porta Proxy:*** porta do Proxy Associado (*Outbound*) para a qual serão direcionadas as mensagens SIP. A porta padrão é a 5060.

- **Opções de Entrada:**
    - **IDC:** permite configurar qual campo da mensagem INVITE do SIP será utilizado como o identificador da chamada (IDC) nas ligações de entrada efetuadas por esse Servidor ao AG 30.

      São disponíveis os campos User(From), que é o caso mais comum, DISPLAYNAME(From), que permite uma identificação mais amigável, porém é um campo não obrigatório, e URI(Contact), que comumente identifica o dispositivo de origem da ligação. O valor que vier no campo selecionado será utilizado nas regras de redirecionamento do VoIP para o TDM nas ligações provindas do domínio desse Servidor SIP. (ver seção: Redirecionamento).

    Obs.: caso for selecionada a opção DISPLAYNAME (From) e o INVITE chegar com esse campo vazio, será utilizado o valor do campo User (From).

- **Usar DDR VoIP:**
    - Campos Display Name, Contact e Restricted ID: Opção utilizada em ligações de saída por operadora VoIP. Permite substituir o valor programado nos campos display name, contact e restricted ID pela identificação de chamada recebida da origem da ligação. Esta configuração tem precedência sobre os valores configurados nos campos de conta. Em casos onde a identificação de chamada da origem for desconhecida são enviados os valores configurados nos campos de operadora.

- **Opções Avançadas:**
  - **DTMF:** Método de transmissão de dígitos DTMF, pode ser dentro ou fora da banda. Quando estiver selecionado dentro da banda o DTMF é enviado com o áudio, podendo apresentar distorções que impossibilitam sua detecção pelo equipamento que irá recebê-lo.
    No DTMF fora da banda é usada a norma RFC2833, onde o dígito é enviado em um pacote RTP.

  - **Codec Preferencial:** compressão de áudio que terá preferência na negociação da chamada. Caso a outra ponta da chamada não suporte a codificação escolhida, outro codec será usado automaticamente.
    - Codecs disponíveis: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps).

  - **Codec (FAX):** Escolha do codec que será usado para a recepção de FAX via VoIP. Para que o T.38 funcione, o aparelho de FAX que irá receber deve estar configurado para recepção automática. Ao enviar um FAX via VoIP é o ponto que recebe o FAX que determina o protocolo a ser usado. Codecs disponíveis: G.711 e T.38.

  - **Protocolo:** Define o protocolo de transporte da sinalização SIP desse servidor. Atualmente tem-se disponível o protocolo UDP.

  - **180 Timeout:** Em alguns casos de ligações recebidas via uma operadora VoIP, o tratamento dessa recepção pode demorar alguns instantes, dependendo para onde a ligação será encaminhada. Esse comportamento atrasa o envio da mensagem SIP 180 (RINGING) para a operadora VoIP, consequentemente atrasando a audição do tom de chamando para quem está efetuando a ligação. Esta configuração permite que seja ajustado um intervalo de espera durante o tratamento da ligação recebida para que o AG 30 envie espontaneamente a mensagem 180 (RINGING) à operadora VoIP. Esse intervalo pode variar entre 0 e 30 segundos.

  - **PRACK:** Habilita a RFC 3262 (Reliable Provisional Responses).

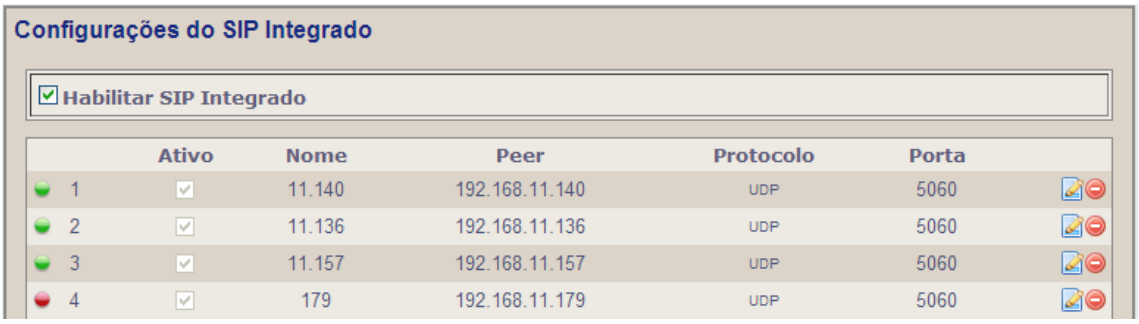
  - **SIP Header Compacto**: Envia as mensagens SIP com headers compactos (RFC 3261 e RFC 6262)

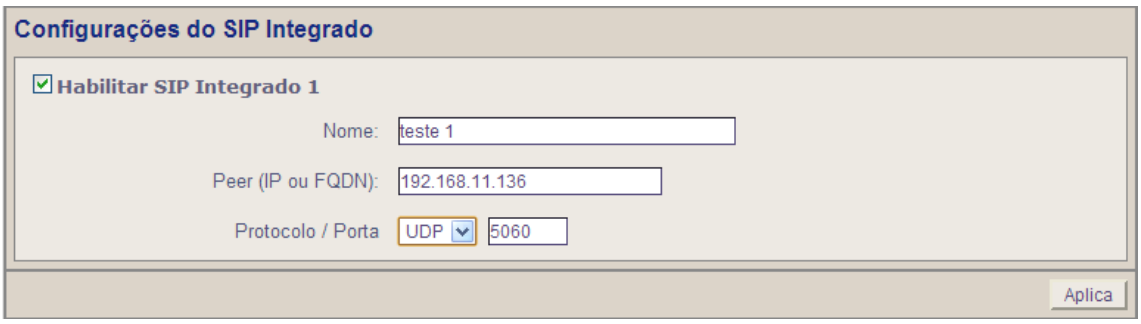
  - **Enviar VAD:** Não envia pacotes ou envia pacotes menores quando detecta silêncio**.**

  - **Usar Codec Remoto:** Nesta opção, durante uma negociação iniciada pelo servidor registrar, o primeiro codec ofertado pelo servidor terá prioridade sobre o codec preferencial configurado.

  - **Enviar SDP em Response 180:** Envio do 180 com SDP e respectivo início de áudio conforme configuração de operadora VoIP.

3.2.2. Configurações SIP Integrado





Objetivo

Funcionalidade que permite interligar equipamentos distintos (pontos) através da interface IP.

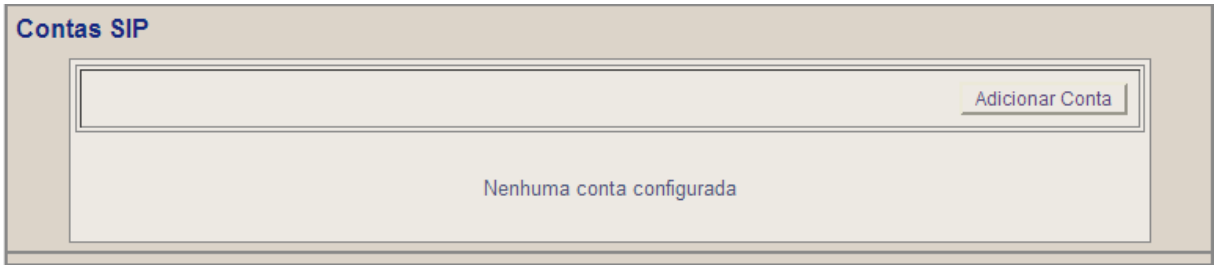
Premissas

Cada ponto será ***independente dos demais***. A configuração de cada ponto será própria, com programações específicas.

O número de pontos remotos máximo é 64.

3.2.2.1. Configurar Contas SIP

Para que seja possível realizar as ligações VoIP é necessário cadastrar as contas SIP e associá-las a um dos servidores SIP cadastrados. É possível cadastrar até 1.000 contas.



- ***Usuário**:* identificação usada para o registro no servidor e nas chamadas VoIP que utilizam o servidor SIP Registrar/Proxy. Este é o campo a ser analisado pela operadora VoIP para identificar o usuário de destino.

- ***Senha**:* usada para a autenticação no servidor SIP Registrar/Proxy.

- ***Display Name**:* campo de texto opcional para identificação do usuário que utiliza a conta.

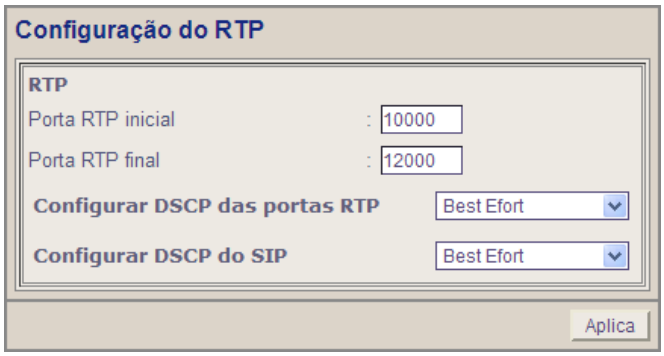
- ***Contact***: ***Login***: usuário usado para autenticar a conta no Servidor SIP. Só é preenchido se o usuário de autenticação for diferente da identificação de registro da conta. Se não for preenchido o AG 30 usa o campo *Usuário* para autenticar a conta.

- ***Restricted ID:*** (texto – identificação adicional): substitui o usuário como identificador. Caso em que o valor "*anonymous*" é enviado para a operadora VoIP, no campo de usuário.

- ***Servidor***: número do servidor SIP Registrar/Proxy onde a conta SIP irá se registrar e encaminhar as ligações.

- ***Permitir ligações simultâneas***: permite ou bloqueia que uma conta SIP, mesmo ocupada, possa fazer outras ligações. Isso evita que o AG 30 fique enviando ligações não permitidas pela operadora, diminuindo o tempo de resposta ao usuário e as mensagens na rede. (Obs.: essa opção não vale para as ligações de entrada, VoIP para TDM, a quais sempre são aceitas, mesmo que a conta SIP esteja ocupada).

3.2.2.2. Configuração de RTP



- **RTP:** Permite especificar o intervalo de portas que será usado para a recepção do áudio. Somente são usadas as portas pares do intervalo.
- Porta RTP inicial: primeira porta do intervalo de portas disponíveis para RTP.
- Porta RTP final: última porta do intervalo de portas disponíveis para RTP.

- **Configurar DSCP das portas RTP**: Permite configurar a prioridade dos pacotes de áudio (RTP) do VoIP (Serviços diferenciados, DiffServ).

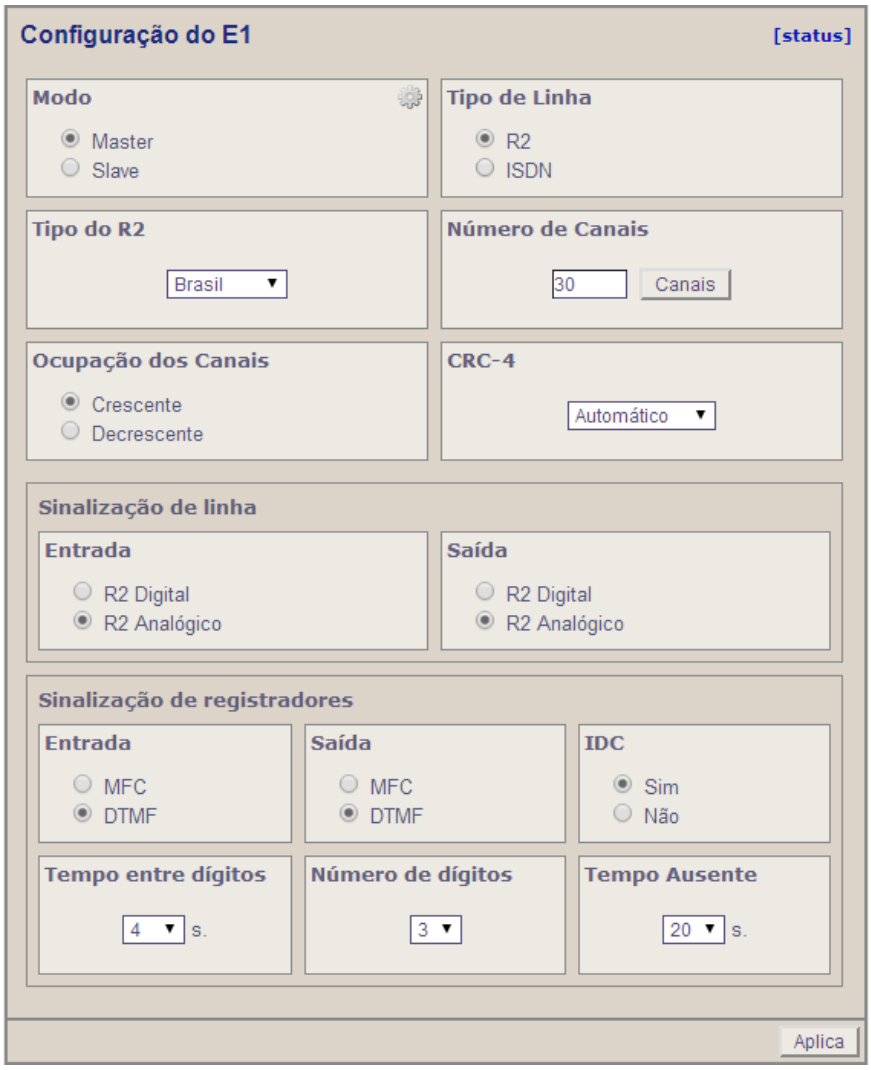
- **Configurar DSCP SIP:** Permite configurar a prioridade dos pacotes do protocolo SIP.

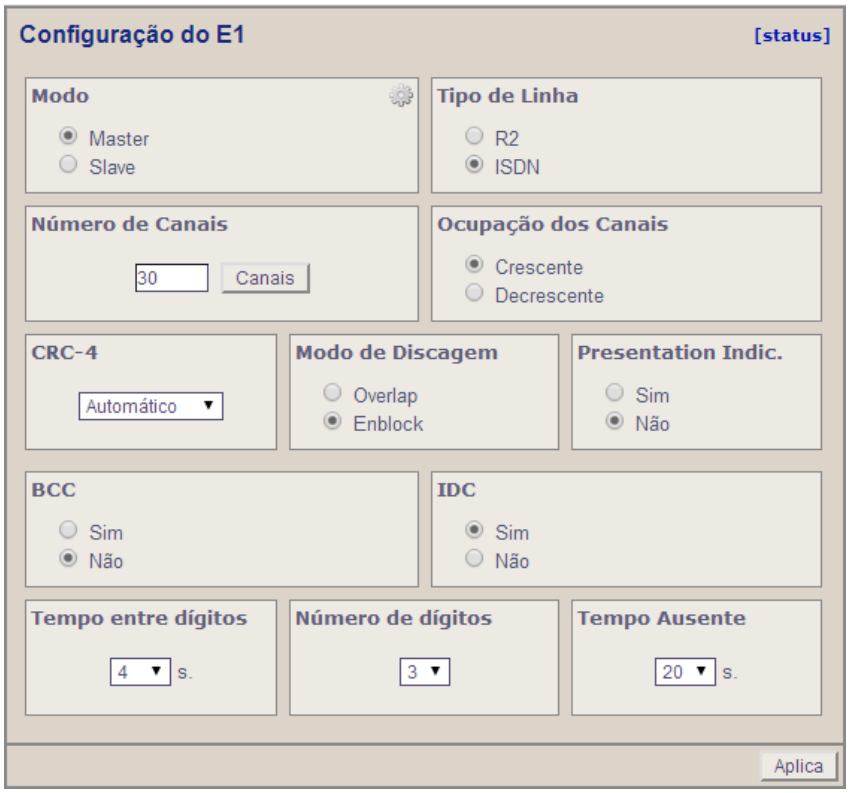
A taxa de amostragem padrão é de 20 ms para o G711 e G729. O cancelamento de eco é de até 128ms.

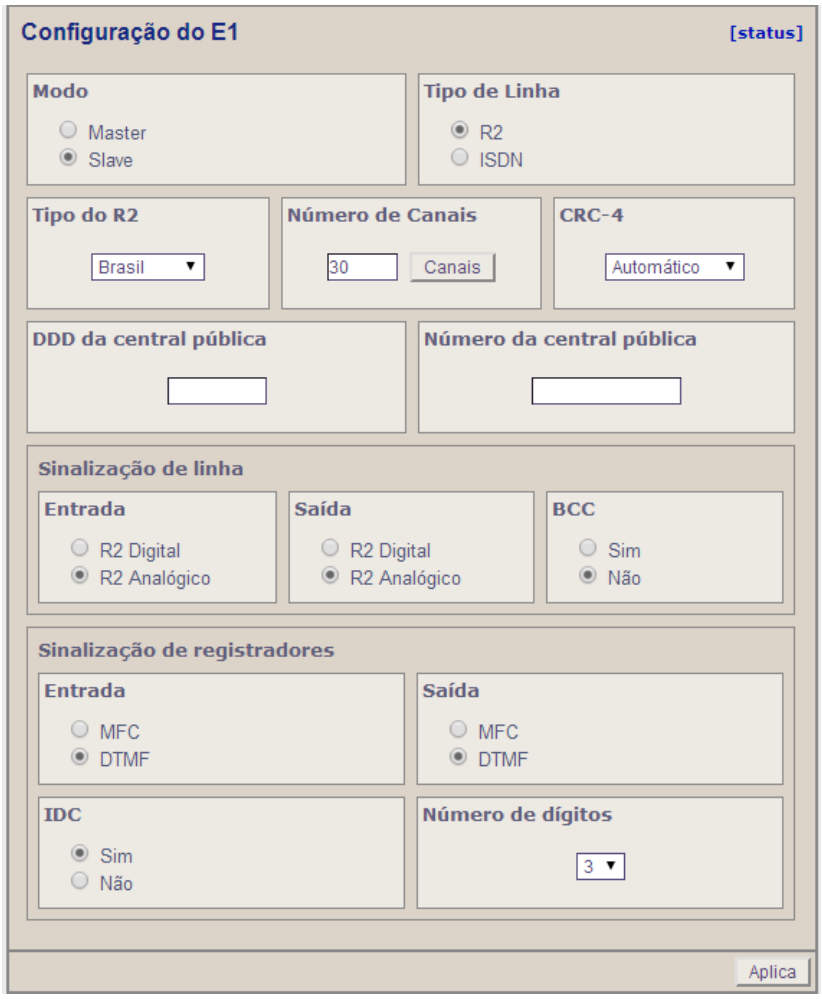
3.3. TDM

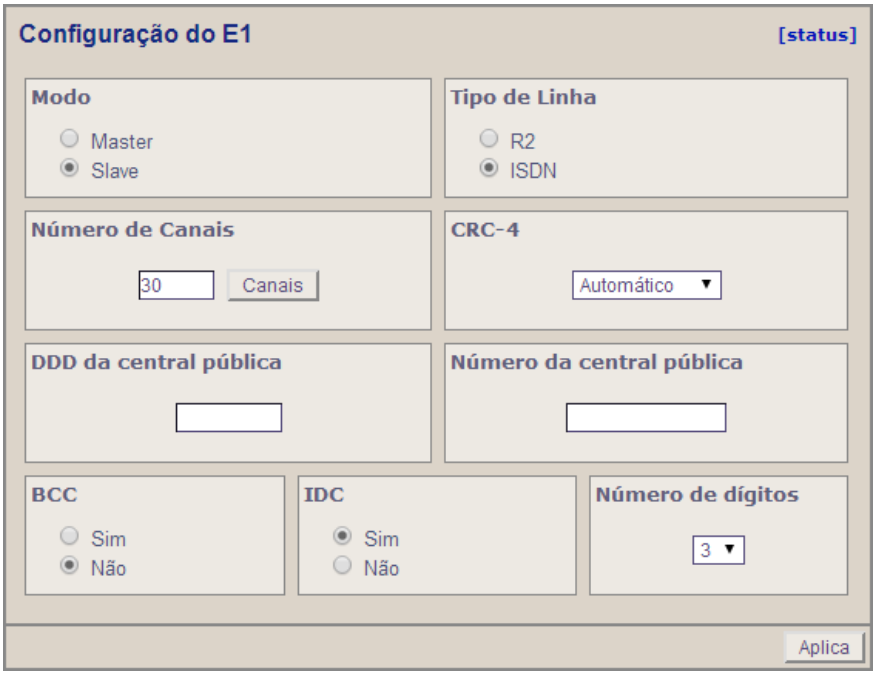
3.3.1. Tronco Digital

A interface E1 necessita ser corretamente configurada, para que a operadora ou PABX e seu AG 30 se comuniquem corretamente.




Configuração do E1
[status]
Modo
Master
Slave
Tipo de Linha
R2
ISDN
Número de Canais
30
Canais
Ocupação dos Canais
Crescente
Decrescente
CRC-4
Automático
Modo de Discagem
Overlap
Enblock
Presentation Indic.
Sim
Não
BCC
Sim
Não
IDC
Sim
Não
Tempo entre dígitos
4
s.
Número de dígitos
3
Tempo Ausente
20
s.
Aplica


Configuração do E1
[status]
Modo
Master
Slave
Tipo de Linha
R2
ISDN
Tipo do R2
Brasil
Número de Canais
30
Canais
CRC-4
Automático
DDD da central pública
Número da central pública
Sinalização de linha
Entrada
R2 Digital
R2 Analógico
Saída
R2 Digital
R2 Analógico
BCC
Sim
Não
Sinalização de registradores
Entrada
MFC
DTMF
Saída
MFC
DTMF
IDC
Sim
Não
Número de dígitos
3
Aplica



Abaixo seguem as descrições de todos os campos configuráveis no E1.

Modo/Tipo de Linha

Esta é a primeira configuração que deve ser feita para o E1.

São disponibilizados dois protocolos para o enlace E1, o R2 e o ISDN. Os protocolos R2 e ISDN podem operar como Master, onde o gateway opera como uma central pública para ser conectado a um PABX, ou como slave para ser conectado a uma operadora. Apenas um destes deve ser selecionado.

Os campos: Tipo de R2, Sinalização de Linha e Sinalização de Registradores ficam desabilitados ao selecionar a opção ISDN.

CRC- 4

CRC - Cyclic Redundancy Check: método de verificação de erros usado em vários protocolos para detecção de erros de transmissão em bits. Pode ser configurado de três modos: habilitado, desabilitado e Automático.

Modo de discagem

Esta configuração possibilita ao AG 30 receber dois tipos de discagem: a Enblock (pacote completo no setup) e Overlap (discagem dígito pelo setup e INFO).

Presentation Indicator

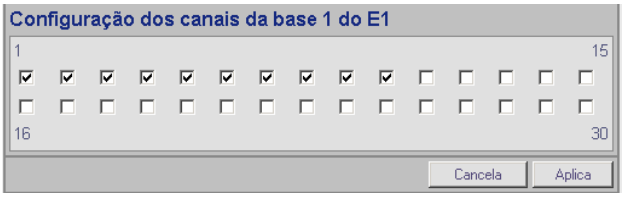
Esta configuração, quando habilitada, é verificado se o PABX está enviando restrição ou não do IDC. Se estiver enviando restrição do IDC, o SIP enviará “anonymous” no campo from.

Tipo de R2

Devido às diferenças de protocolos utilizados, para o correto funcionamento da sinalização MFC e particularidades do envio de IDC, este campo deve ser selecionado.

Número de canais

Neste campo deve ser configurado o número de canais contratados com a prestadora, sendo assim a configuração do seu E1 é flexível conforme o desejado.



Ocupação dos Canais

Define se a ocupação dos canais do E1 no AG 30 será crescente ou decrescente. Se for configurado como crescente, será escolhido sempre o menor canal E1 disponível para encaminhar ligações para o equipamento conectado à interface E1. Caso for escolhida a opção "decrescente", o gateway selecionará sempre o maior canal disponível. Isso permite diminuir a chance de colisões, uma vez que ao definir uma ordem diferente da utilizada no PABX conectado ao AG 30, ocorrerá uma colisão somente quando todos os canais forem ocupados.

DDD da Central Pública

Informar neste campo o código DDD do local da instalação.

Sinalização de Linha

Pode ser configurada tanto para entrada como para saída independentemente. A configuração pode ser feita entre R2 analógico (também conhecida como E+M contínua) ou R2 digital. A sua correta configuração deve estar de acordo com sua prestadora.

BCC: Habilita/Desabilita a função de BCC, funcionalidade disponível no E1 modo Slave. Caso o BCC seja habilitado não poderão entrar chamadas a cobrar. Neste caso, se entrar uma chamada a cobrar o Gateway automaticamente derrubará a mesma após o atendimento.

Tempo entre dígitos

Apenas utilizado no modo master. Define o tempo máximo de espera entre os dígitos do número de destino enviados pelo PABX ao AG 30 no protocolo E1 (R2/MFC). Se expirar o tempo máximo para enviar o dígito seguinte, a sequencia digitada pelo executor da chamada será considerada finalizada. Caso esta sequência não for equivalente a nenhuma regra de dígitos da Resolução 86 da Anatel, então o critério de análise para o término da sequência será o tempo desta configuração. Ainda, se o início desta sequência atender a uma regra da Resolução 86, mas não for fornecido o número de dígitos esperados, também a ligação será encaminhada após expirar o tempo entre dígitos.

Número de dígitos

No modo master deve ser definido o número de dígitos recebidos a serem encaminhados. Por exemplo, se forem configurados 4 dígitos e o número de destino recebido na ligação for 3590-3456, os dígitos enviados serão os últimos 4, i.e., 3456. (Obs.: a quantidade de dígitos pode ser menor dependendo das regras definidas na configuração de redirecionamento. Ver seção "Configuração do Redirecionamento de Chamadas"). No modo slave este campo serve para indicar ao gateway quantos dígitos deve requisitar da operadora nas ligações de entrada.

IDC - Identificador de Chamadas

Quando ativado no modo master, o AG 30 irá pedir ao PABX a ele conectado o número de identificação de quem está realizando a chamada (IDC). Para o correto funcionamento, o PABX deve também ser configurado para o envio do IDC. Uma vez recebido pelo Gateway, o IDC será repassado ao destino da ligação. No modo slave o gateway irá enviar o número configurado pela regra de redirecionamento quando solicitado pela operadora.

Envia fim de Discagem (apenas E1 Argentina)

Após o envio do último número de destino por parte do AG 30, e no caso de que a pública solicite um dígito a mais, deverá ser enviado um sinal MFC "IF" informando o fim da discagem. Este sinal é utilizado para indicação de fim de IDC, mas que aqui será utilizado também para indicar o fim da discagem.

Envia ANI (apenas E1 Argentina)

Envia o ANI para a central pública possibilitando a tarifação por DDR.

Envia IDC (apenas E1 Argentina)

Permite que a central pública envie IDC ao número de destino.

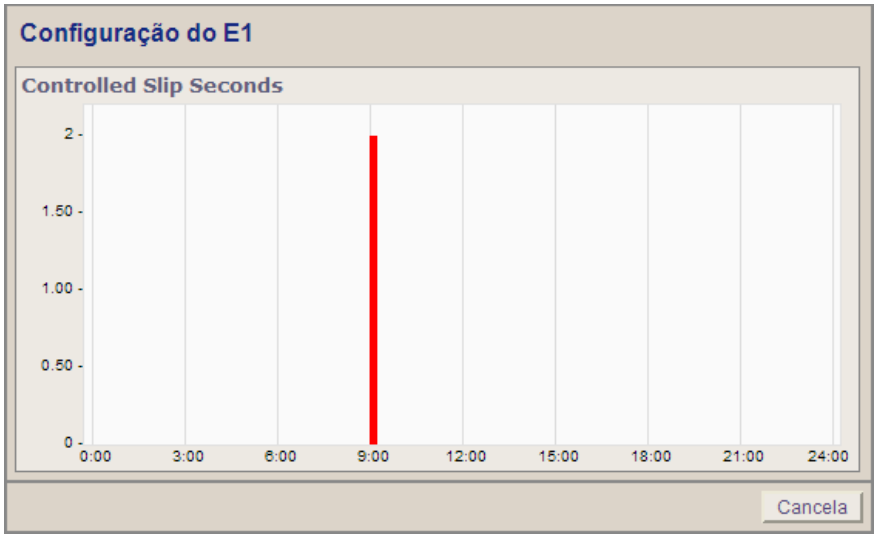
3.3.1.1. Status

Permite a visualização dos status do link e1. Quando o link estiver sem a presença de alarmes aparecerá “Link Status up”. Caso contrário “Link Status down”.

Além disso, é possível verificar estatísticas de erros dos últimos 15 minutos e também o histórico das últimas 24 horas. Clicando na opção “more” um gráfico mostrará a ocorrência de erros de 15 em 15 minutos das últimas 24 horas.

As estatísticas estão definidas na RFC 4805 “Definitions of Managed Objects for the DS1, J1, E1, DS2, and E2 Interface Types”.

Configuração do E1
Last 15min
Last 24h
Errored Seconds 0 2 more...
Severely Errored Seconds 0 2 more...
Severely Errored Framing Seconds 0 2 more...
Unavailable Seconds 0 0 more...
Controlled Slip Seconds 0 2 more...
Path Coding Violations 0 0 more...
Line Errored Seconds 0 0 more...
Bursty Errored Seconds 0 0 more...
Line Code Violations 0 0 more...
Link Status up
Cancela



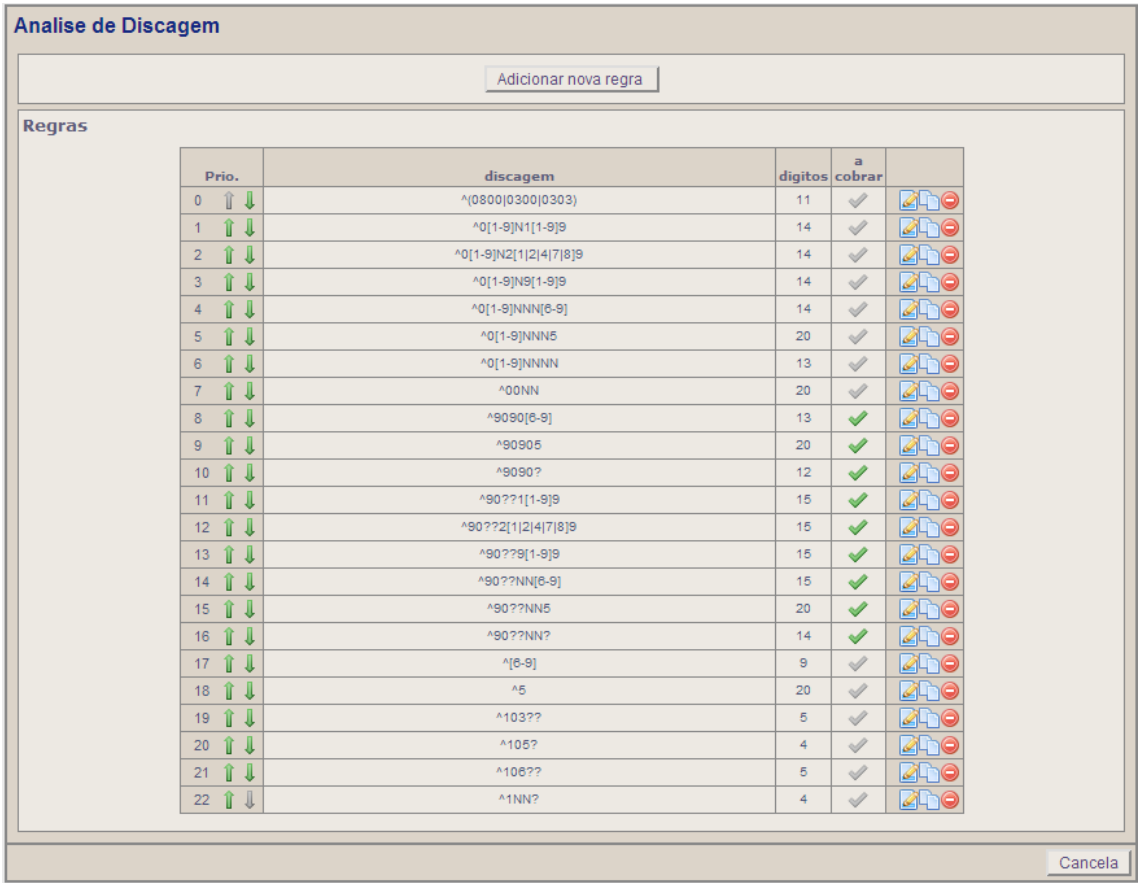
3.3.1.2. Analise de Dígitos (E1 Master)

Nas ligações de entrada via E1 (Master) a discagem é analisada dígito a dígito. Quando a discagem corresponder a alguma regra da tabela de análise de discagem, será definido o número de dígitos até o encaminhamento da chamada. Isto quer dizer que, quando este número de dígitos for alcançado, a ligação será encaminhada sem aguardar o time out de discagem pelo usuário. Desta forma a discagem ocorrerá de forma mais rápida..

A tabela de discagem é pré-definida em fábrica, podendo ser alterada pelo usuário para customizar as ligações de acordo com a sua localidade.

Esta tela é acessada via configurador web em "TDM→ Tronco Digital", quando o tronco digital estiver configurado no modo "Master".

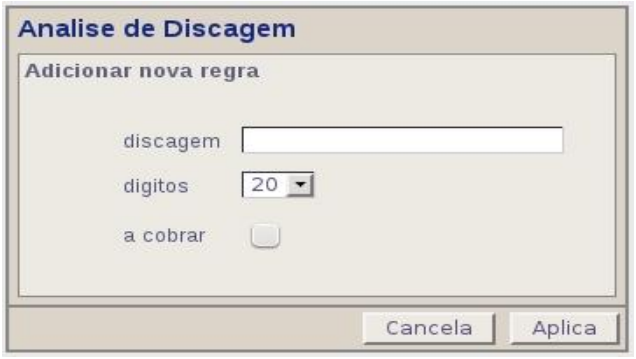
3.3.1.2.1. Tabela de analise de discagem:



Prio.	discagem	digitos	a cobrar
0	^(0800|0300|0303)	11	
1	^0[1-9]N1[1-9]9	14	
2	^0[1-9]N2[1|2|4|7|8]9	14	
3	^0[1-9]N9[1-9]9	14	
4	^0[1-9]NNN[6-9]	14	
5	^0[1-9]NNN5	20	
6	^0[1-9]NNNN	13	
7	^00NN	20	
8	^9090[6-9]	13	✓
9	^90905	20	✓
10	^90907	12	✓
11	^90??1[1-9]9	15	✓
12	^90??2[1|2|4|7|8]9	15	✓
13	^90??9[1-9]9	15	✓
14	^90??NN[6-9]	15	✓
15	^90??NN5	20	✓
16	^90??NN7	14	✓
17	^[6-9]	9	
18	^5	20	
19	^103??	5	
20	^1057	4	
21	^106??	5	
22	^1NN7	4	

- **Prio.**: Prioridade das regras em ordem crescente. A discagem será verificada regra a regra até coincidir em uma delas.
- **discagem**: Regra para análise.
- **dígitos**: Número de dígitos esperados para o tipo de discagem.
- **a cobrar**: Indica se o tipo de discagem corresponde a uma ligação a cobrar ou não (utilizado apenas para ligações de entrada VoIP).

3.3.1.2.2. Adicionar nova regra:

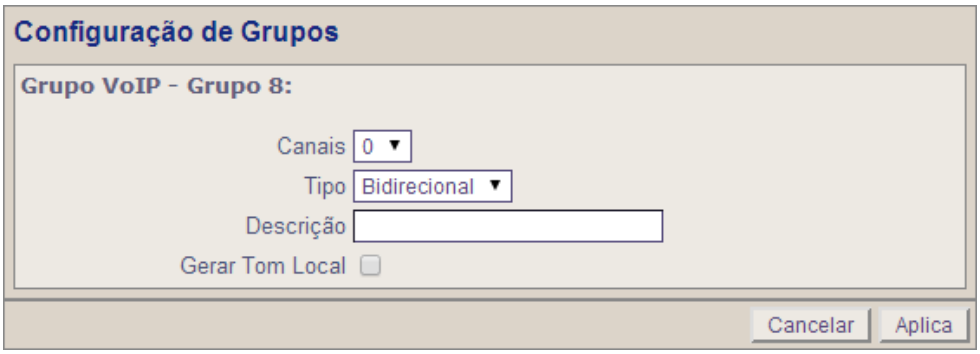


- **discagem**: Expressão regular para analise da
- **dígitos:** Número de dígitos esperados para o **tipo de** discagem.
- **a cobrar**: Indica se o tipo de discagem corresponde a uma ligação a cobrar ou não (utilizado apenas para ligações de entrada VoIP).

3.3.2. Grupos

Para cada tipo de canal no AG 30 (VoIP ou E1), podem ser configurados até 10 grupos. Estes grupos serão utilizados nas regras de redirecionamento. No caso de grupos E1 e VoIP para cada grupo é definido a quantidade de canais por grupo, ou seja um range de canais para cada grupo.

No campo “Tipo” é possível determinar se os canais do grupo são definidos como somente entrada, somente saída ou bidirecional, e se o grupo deve gerar Tom Local ou não. Já o campo descrição serve para colocar uma identificação ao usuário sobre a utilidade do grupo para auxiliar na programação das regras de redirecionamento.



3.3.2.1. Tom Local

Grupo E1 - Gerar Tom Local - Esta configuração habilita o tom local no sentido: PABX AG 30 → VoIP, caso o lado VoIP não envie o tom de chamando o AG 30 irá enviar o tom.

Grupo VOIP - Gerar Tom Local - Está configuração habilita o tom local no sentido: VoIP → AG 30 → PABX , caso o lado do PABX não envie o tom de chamando o AG 30 irá enviar o tom.

3.3.3. Redirecionamento

O correto funcionamento do AG 30 está baseado na programação das regras de redirecionamento de chamadas. A partir da análise das informações das ligações recebidas será feito o tratamento das ligações de saída. De modo a redirecionar as ligações entre as interfaces (TDM e VoIP) é necessário fazer a associação dos números de FROM e TO. Assim, uma ligação recebida ou realizada por um interface utilizará o seu par na outra interface.

Esses redirecionamentos são configurados utilizando-se de regras com expressões regulares[1], as quais permitem realizar a associação e substituições de modo flexível.

Redirecionamento de Chamadas
Adicionar nova regra
Regras
Ligações Recebidas:
Encaminhar por:
Prio. I.Entrada From To Grupos I.Saída From To Grupos
0 Op.VoIP * 5140638498 0 E1 {From} 5000 0
1 E1 * 5002 0 S.Int:1 {From} 3202 0
2 S.Int:3 * ^0 0 Op.VoIP 5140638498 {To:1} 0

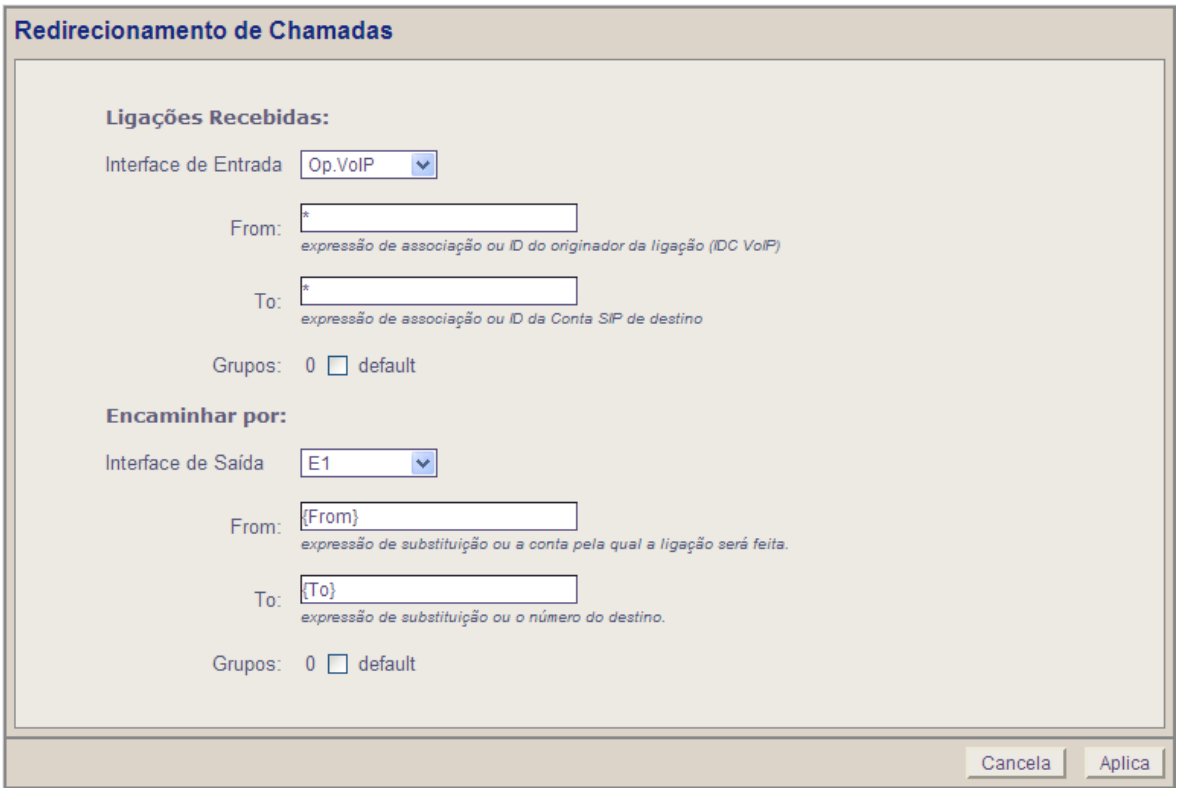
3.3.3.1. Adicionar Regra

Uma nova regra é inserida através do botão “Adicionar nova regra”.

Os botões à direita servem para Alterar, Duplicar ou Remover uma regra existente. O botão “Alterar” edita a regra selecionada abrindo a possibilidade de alterar também a sua prioridade, o botão “Duplicar” cria uma regra idêntica e logo abaixo da regra selecionada, o botão “Remover” remove a regra selecionada.

O AG 30 permite alterar a ordem de execução das regras de acordo com a necessidade do usuário, através das setas laterais ou ainda através da opção “Alterar” onde é possível alterar diretamente a prioridade da regra.

[1] Expressões regulares: provém, por meio de uma linguagem formal, uma maneira concisa e flexível para identificar cadeias de caracteres de interesse, como caracteres específicos, palavras, ou padrões de caracteres.


Redirecionamento de Chamadas
Ligações Recebidas:
Interface de Entrada
Op.VoIP
From:
*
expressão de associação ou ID do originador da ligação (IDC VoIP)
To:
*
expressão de associação ou ID da Conta SIP de destino
Grupos:
0
default
Encaminhar por:
Interface de Saída
E1
From:
{From}
expressão de substituição ou a conta pela qual a ligação será feita.
To:
{To}
expressão de substituição ou o número do destino.
Grupos:
0
default
Cancela
Aplica

LIGAÇÕES RECEBIDAS:

Para adicionar uma regra devemos definir as informações da ligação de entrada. Primeiramente a origem. No campo “Interface de entrada” podemos escolher entre os tipos:

- Op. Voip – Operadora VoIP
- Sip Int. – Sip integrado (1 até 64)
- E1 – Entroncamento digital tipo E1 R2 ou ISDN

Definida a interface de entrada é necessário definir o “from” e o “to”. Estes campos possuem significados diversos dependendo do tipo de entrada e da posição onde o mesmo foi colocado:

Ex1. Entrada Tipo E1 conectado a uma operadora:

- From = DDD + 8 ou 9 dígitos do número de origem
- To = DDR de 3 ou 4 dígitos

Ex2. Entrada SIP Integrado conectado a um Pabx:

- From – Número de um ramal do PABX remoto
- To – Número da PSTN

Além destes campos, o grupo do canal de entrada da ligação é analisado para auxiliar no encaminhamento da ligação. Com isto é possível fazer reserva de canais para entrada de ligações e encaminhamento dependente da operadora de entrada.

ENCAMINHAR POR :

Após definidas as condições de análise da ligação de entrada, é necessário definir a saída da ligação.

Da mesma forma que na entrada, deverá ser escolhida a interface de saída. Para ligação de saída existe a opção de mais uma interface que é a “DISA”. Esta opção direciona a ligação de entrada para uma mensagem gravada. Durante esta mensagem o usuário poderá discar até 20 dígitos. Depois de encerrada a discagem, o AG 30 captura estes números e aplica novamente as regras de redirecionamento. As demais opções de interface de saída são idênticas as da entrada. Não é permitida a interligação entre entrada E1 para saída E1, e entrada Op. VoIP para saída Op.VoIP. É permitido apenas o caso entrada Sip Int. para saída Sip Int.

Já os campos From e To podem ser manipulados para envio ao destino. É possível substituir, incluir ou excluir, parcial ou totalmente, os números recebidos na entrada. Isto se dá através do uso de expressões regulares.

Ex. Uma ligação chega no AG 30 através da Interface de Entrada Sip Int 1 com número de From 266 e To 035792200. Ela deverá ser encaminhada para o E1 com From = 513792 + DDR e sem o "0" no To.

Utilizando expressões regulares devemos configurar:

- From = 5135792{From}
- To = {To:1}

O Grupo deverá ser escolhido de acordo com o critério desejado pelo usuário. É possível fazer um balanceamento de chamadas reservando canais para um determinado tipo de entrada/saída.

3.3.3.2. Expressões de Associação

As expressões de associação são utilizadas para descreverem as ligações de entrada. Elas são baseadas nas expressões regulares e permitem vincular com uma ou várias ligações. Para isso, pode-se combinar os seguintes comandos:

^	Início da discagem
N	Um dígito: [0-9], [a-z] ou [A-Z]
*	Nenhum ou mais dígitos N
+	Um ou mais dígitos N
?	Nenhum ou um dígito
[x-y]	Intervalos como: [1-3], [a-z]...
[1,4]	Somente dígitos: 1 e 4
$	Fim da discagem
{n,m}	De 'n' a 'm' caracteres
{n}	Exatamente 'n' caracteres

Exemplos:

^NNN	Qualquer número de três dígitos (ex.: 201, 356, 999, etc)
^2NN	Qualquer número de três dígitos, iniciado com 2 (ex.: 201, 205, 209, etc)
^[0-8]	Qualquer número cujo o primeiro dígito esteja entre 0 e 8, isto é, excluindo os que começam com o dígito 9 (ex.:0800, 30303030, 07711.., etc)
*	Qualquer número. (ex.: 201, 9090303030, 0800, etc)

3.3.3.3. Expressões de Substituição

As expressões de substituição são utilizadas no encaminhamento das ligações, trocando dígitos ou caracteres para os valores equivalentes na outra interface. A seguir tem-se a sintaxe dessas expressões:

- Expressão de substituição do originador: <num>{From:<offset>:<length>}<num>
- Expressão de substituição de destino: <num>{To:<offset>:< length >} <num>

Com essas expressões é possível referenciar os números originais pelas palavras "From" para o originador e "TO" para o destino. Podem-se acrescentar números antes ou depois (<num>) e também referenciar somente partes dos números originais, possibilitando uma gama de combinações. A referência para parte dos números originais (From ou To) é feita apontando o primeiro digito em <offset> e quantos dígitos, a partir do primeiro, que serão considerados em <length>. Existem algumas considerações:

- O primeiro dígito está na posição zero (offset = 0).
- O offset considera-se da esquerda para a direita.
- Se a length for omitido, então todo o restante dos dígitos, iniciando do offset, será considerado.
- Se offset for omitido e a length for negativo, são considerados os dígitos da direita para a esquerda.
- Quando for utilizado offset e length negativo simultaneamente, temos um intervalo, onde length serem desconsiderados da direita para esquerda (atua como um offset no sentido inverso).

Exemplos:

Sendo "To" igual a "30405060", têm-se os seguintes resultados com as expressões abaixo:

{To:4}	Significado: a partir do dígito na posição quatro, pega todo o resto. Resultado: 5060
{To:0:3}	Significado: a partir do dígito na posição zero, pega três dígitos. Resultado: 304
09988{To}	Significado: acrescenta o prefixo 09988. Resultado: 0998830405060
{To:2:-1}	Significado: pega o intervalo a partir do dígito na posição dois e retira o último algarismo do número. Resultado: 40506

Sendo "From" igual a "2345", têm-se os seguintes resultados com as expressões abaixo:

{From:-3}	Significado: a partir da direita, pega três dígitos. Resultado: 345
30{From}40	Significado: acrescenta o prefixo 30 e o sufixo 40. Resultado: 30234540

3.3.3.4. Ordem de execução das regras:

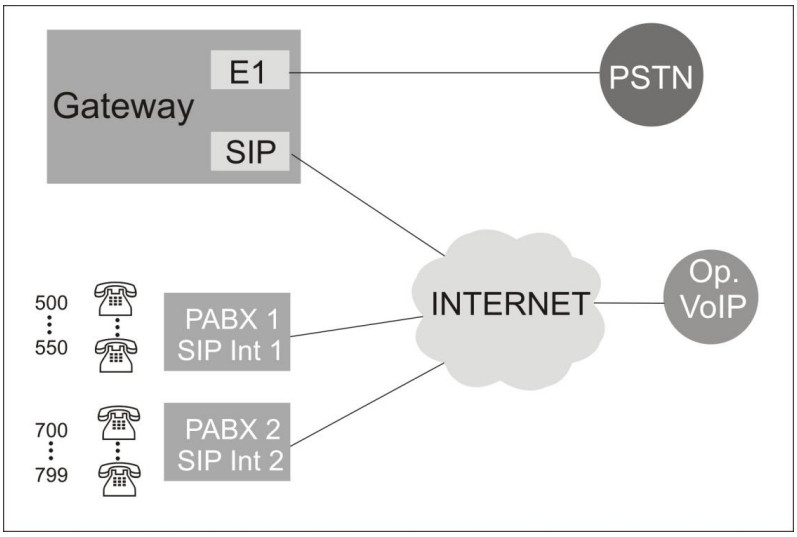
A ordem de execução das regras influência no resultado final. As regras mais prioritárias são as de valor mais baixo, ou seja, a ordem de prioridades é do menor ao maior. As novas regras adicionadas vão para o fim da lista de regras.

3.3.4. Casos de uso

Para fins de exemplo iremos estabelecer sempre o ponto de vista da interface conectada a um usuário ou PABX como origem ou destino. Isto facilita a elaboração dos exemplos de regras de redirecionamento.

3.3.4.1. Caso 1

Usuários conectados através de Sip Integrado. E1 e Op.VoIP conectado a operadoras de telefonia.



No nosso exemplo o AG 30 deverá permitir que os ramais das centrais PABX dos Sip Integrado 1 e 2 da figura deverão poder realizar os seguintes tipos de ligações:

Ligações de Saída a partir do SIP integrado 1:

- **Regra 0** - Ligações para o DDD 11 deverão ser encaminhadas através do E1 utilizando a operadora de número “21”

- **Regra 1** - Ligações para os números 35792250 até 35792299 deverão ser encaminhados para os ramais do Sip Integrado 2.

- **Regra 2** - Ligações DDD para as demais localidades deverão ser encaminhadas para a Op. VoIP 1 na conta "filial1". O número de destino deverá incluir 55+DDD na frente do número para que a operadora VoIP complete a ligação.

- **Regra 3** - Demais ligações através do E1.

Ligações de Entrada para o Sip Integrado 1:

- **Regra 4** - Ligações E1 para os DDRs de 200 até 249 deverão ser encaminhadas para os ramais 500 a 549

Ligações de Saída a partir do SIP Integrado 2

- **Regra 5** - Ligações para o DDD 11 deverão ser encaminhadas através do E1 utilizando a operadora de número "21"

- **Regra 6** - Ligações DDD para os números 35792200 até 35792249 deverão ser encaminhados para os ramais do Sip Integrado 1.

- **Regra 7** - Ligações DDD para as demais localidades deverão ser encaminhadas para a Op. VoIP 1 na conta "filial2". O número de destino deverá incluir 55+DDD na frente do número para que a operadora VoIP complete a ligação.

- **Regra 8** - Demais ligações através do E1

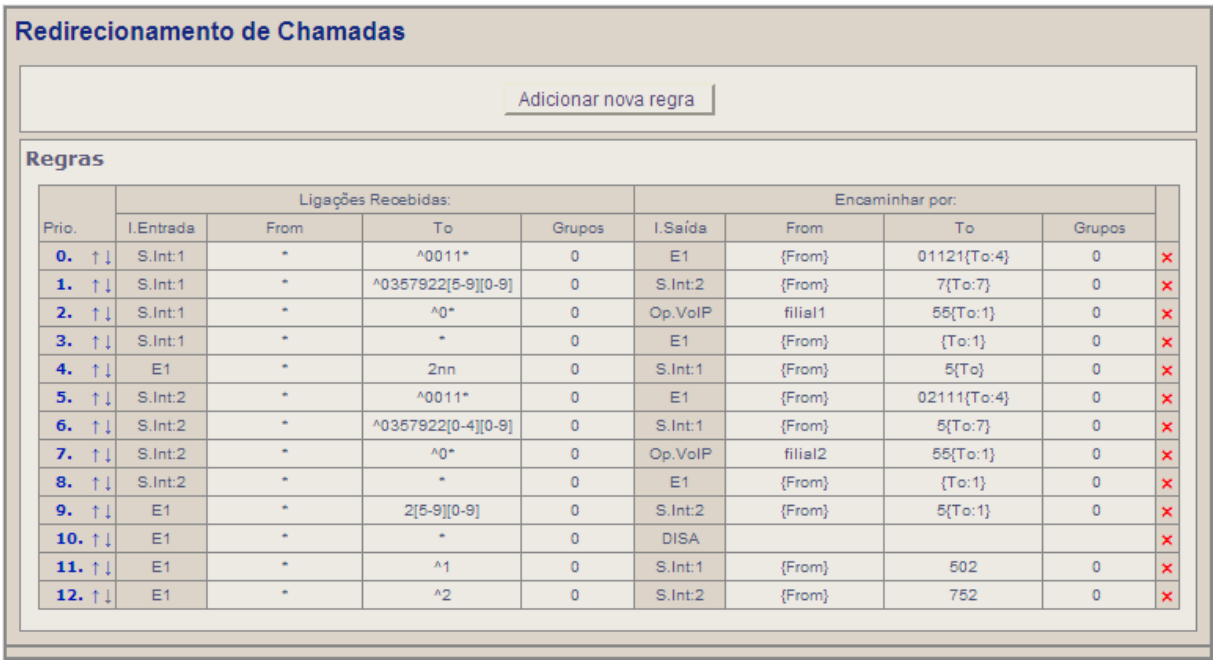
Ligações de Entrada para o Sip Integrado 2:

- **Regra 9** - Ligações E1 para os DDRs de 250 até 299 deverão ser encaminhadas para os ramais 500 a 549

Ligações DISA:

- **Regra 10 e 11** – Ligações de entrada através do E1 que não encontrarem correspondência em nenhuma regra anterior deverão ser encaminhadas para o DISA. No DISA caso seja discado apenas o dígito "1" a ligação deverá ser encaminhada para o ramal 502 do Sip Int 1.

- **Regra 12** – Ligações de entrada através do E1 que não encontrarem correspondência em nenhuma regra anterior deverão ser encaminhadas para o DISA. No DISA caso seja discado apenas o dígito "2" a ligação deverá ser encaminhada para o ramal 702 do Sip Int 2.



Redirecionamento de Chamadas

Adicionar nova regra

Regras

Prio.	Ligações Recebidas: I.Entrada	From	To	Grupos	Encaminhar por: I.Saída	From	To	Grupos	
0. ↑↓	S.Int:1	*	^0011*	0	E1	{From}	01121{To:4}	0	×
1. ↑↓	S.Int:1	*	^0357922[5-9][0-9]	0	S.Int:2	{From}	7{To:7}	0	×
2. ↑↓	S.Int:1	*	^0*	0	Op.VoIP	filial1	55{To:1}	0	×
3. ↑↓	S.Int:1	*	*	0	E1	{From}	{To:1}	0	×
4. ↑↓	E1	*	2nn	0	S.Int:1	{From}	5{To}	0	×
5. ↑↓	S.Int:2	*	^0011*	0	E1	{From}	02111{To:4}	0	×
6. ↑↓	S.Int:2	*	^0357922[0-4][0-9]	0	S.Int:1	{From}	5{To:7}	0	×
7. ↑↓	S.Int:2	*	^0*	0	Op.VoIP	filial2	55{To:1}	0	×
8. ↑↓	S.Int:2	*	*	0	E1	{From}	{To:1}	0	×
9. ↑↓	E1	*	2[5-9][0-9]	0	S.Int:2	{From}	5{To:1}	0	×
10. ↑↓	E1	*	*	0	DISA				×
11. ↑↓	E1	*	^1	0	S.Int:1	{From}	502	0	×
12. ↑↓	E1	*	^2	0	S.Int:2	{From}	752	0	×

Com isto é possível exemplificar um caso típico de uso onde os PABX 1 e 2 se comunicam entre si através do VoIP, sem custo de ligação, os número fornecidos pela operadora E1 são divulgados para acesso a todos os usuários e os custos de ligação DDD e celular são otimizados através dos usos da Op. VoIP.

Para tanto devemos fazer regras onde o destinatário receba como IDC da ligação o número divulgado para retorno através do E1, ou seja, 1135792 + DDR, independente da interface de saída.

3.3.4.2. Caso 2

Usuários conectados a um PABX legado (sem interface VoIP) através do E1 e Op. VoIP conectadas a operadoras de telefonia.

Ligações de saída através do E1:

- **Regra 0** – Ligações para os números 35792200 até 35792299 direcionados para os ramais do PABX do sip integrado 1.

- **Regra 1** - Ligações DDD através do Op Voip 1 inserindo 025+DDD pela conta “matriz”.

- **Regra 2** – Ligações locais através da Op. VoIP 1 inserindo 02511 pela conta “matriz”.

Ligações de Entrada para o PABX conectado ao E1:

- **Regra 3** – Ligações recebidas da Op. Voip com to de 30305000 até 30305099 deverão ser encaminhadas os DDRs do E1 no range 500 até 599.

- **Regra 5** - Ligações recebidas do SIP Integrado 1 com números 1130305000 até 1130305099 deverão ser encaminhadas os DDRs do E1 no range 500 até 599.

Ligações de Entrada a partir dos Sips Integrados:

- **Regra 5** - Toda ligação de saída vindas dos SIPs integrados 2,3 e 5 até 9 serão efetuadas através da Op. VoIP pela conta "matriz".

Redirecionamento de Chamadas

Adicionar nova regra

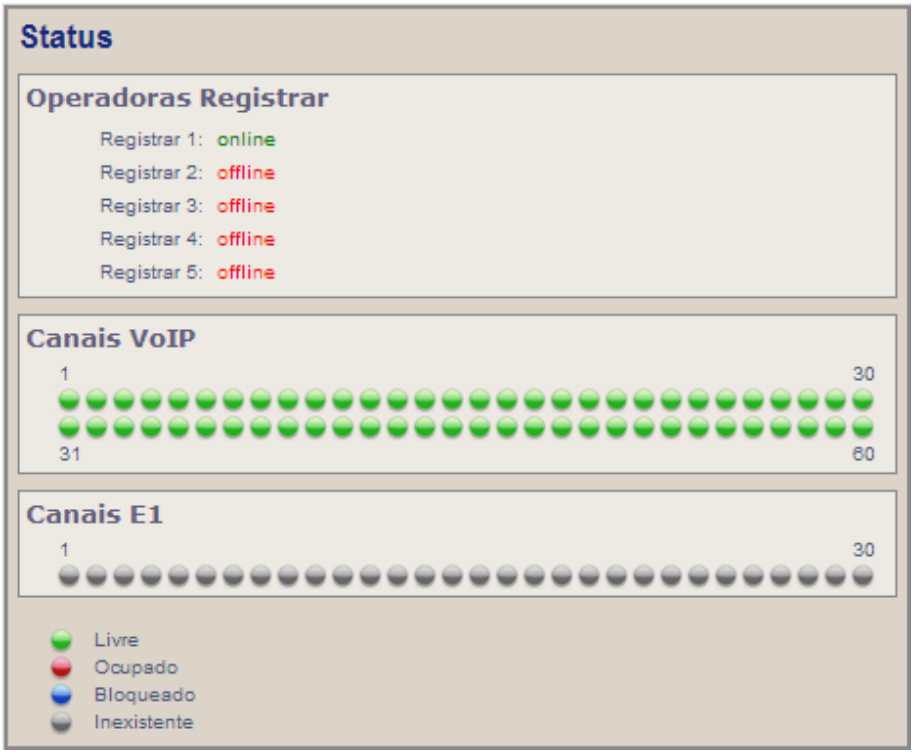
Regras

Prio.	Ligações Recebidas:				Encaminhar por:				
	I.Entrada	From	To	Grupos	I.Saída	From	To	Grupos	
0. ↑↓	E1	*	^357922nn	0	S.Int:1	{From}	{To:5}	0	×
1. ↑↓	E1	*	^0*	0	Op.VoIP	matriz	025{To:1}	0	×
2. ↑↓	E1	*	*	0	Op.VoIP	matriz	02511{To}	0	×
3. ↑↓	Op.VoIP	*	51303050nn	0	E1	{From}	5{To:8}	0	×
4. ↑↓	S.Int:1	*	^11303050nn	0	E1	{From}	5{To:8}	0	×
5. ↑↓	S.Int:2-3,5-9	*	*	0	Op.VoIP	matriz	{To:1}	0	×

O caso 2 é um exemplo típico de integração de um PABX legado (sem VoIP) com o mundo IP.

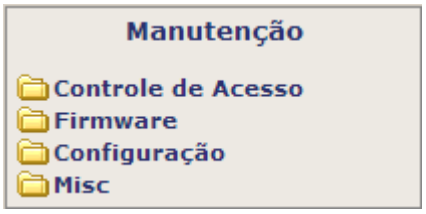
3.3.5. Status

O AG 30 atualiza a cada 10 segundos a tela de status dos canais. Os canais livres estão na cor verde, os ocupados em vermelho, os bloqueados em azul e os inexistentes em cinza. Também é possível verificar por esta o estado das Operadoras Registrar.



3.4. Manutenção

Os itens a seguir são para realizar a manutenção do sistema depois de configurado.

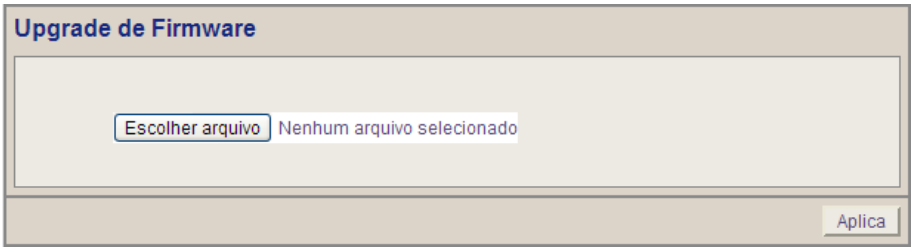


3.4.1. Firmware

3.4.2. Versões

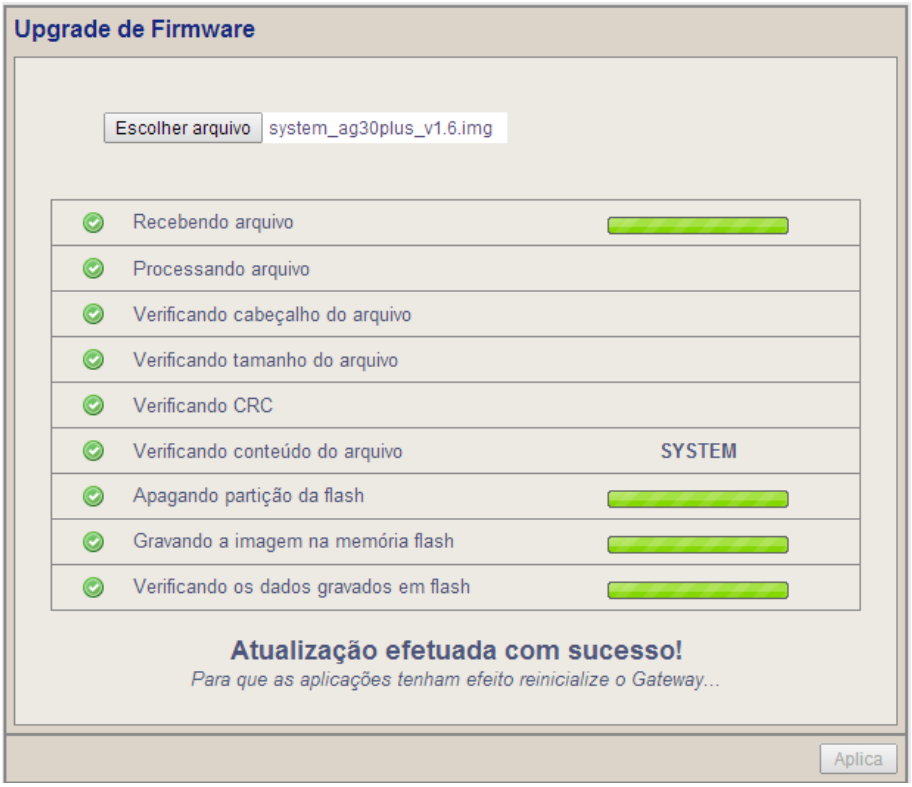
3.4.3. Upgrade de Firmware

Para manter seu AG 30 sempre atualizado existe na opção upgrade de firmware, uma forma bastante simples de operação. Colocando no campo “Upgrade de Firmware”, qualquer pacote de atualização (System, SIP ou Xilinx), o AG 30 irá automaticamente identificar o pacote utilizado e efetuar a gravação do novo pacote.



Se a gravação ocorrer com sucesso, você deve reiniciar o AG 30. Caso haja algum problema, verifique se a imagem não está corrompida, e repita a operação. Para que haja mais segurança a atualização deve ser feita por uma máquina da interface LAN, embora seja possível atualizar pela interface WAN, habilitando o campo respectivo nas configurações gerais do firewall (Ver *“Seção Firewall”*).

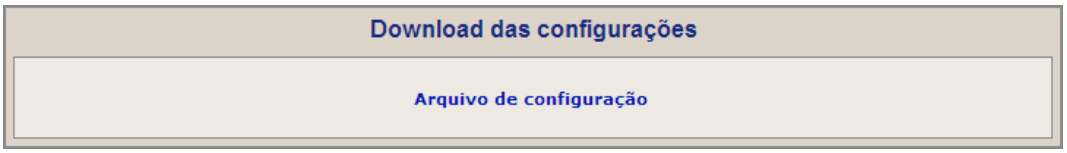
OBS.: *Durante o processo de atualização do firmware alguns serviços podem parar de funcionar. Para o restabelecimento de todas as de todas as funções, aguarde a atualização e resete o AG 30.*



3.4.4. Configuração

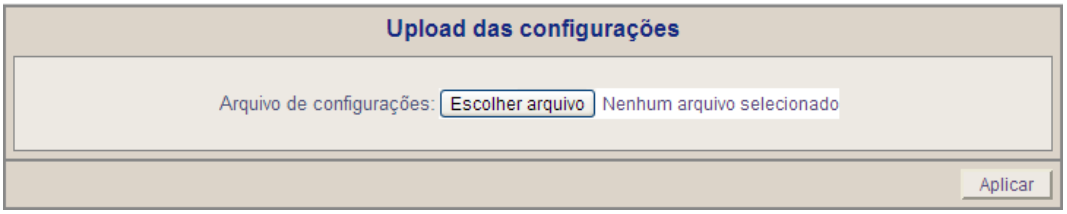
3.4.5. Download

Permite fazer um backup dos arquivos de configuração. Após clicar em download e digitar a senha de programação correta, aparecerá uma tela que permite realizar o download do arquivo de configuração do AG 30, para um diretório a sua escolha em seu computador.



3.4.6. Upload

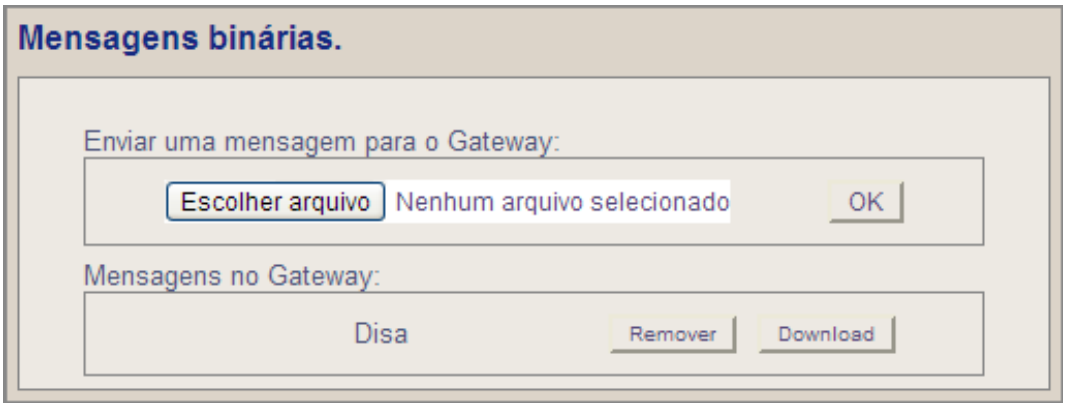
Permite a partir de um backup do arquivo de configuração, voltar a uma configuração feita anteriormente. Após clicar em upload aparecerá uma tela que permite realizar o upload do arquivo de configuração. Procure o diretório do computador, onde está o arquivo baixado anteriormente e clique em “Aplica” para trazer o arquivo do computador para o AG 30. Para as modificações terem efeito será necessário desligar e ligar o AG 30.



3.4.7. Misc

3.4.8. Mensagens Binárias

A mensagem binária DISA é uma mensagem de auxílio ao usuário.



Enviar uma mensagem para o Gateway

Em "Procurar..." escolha o arquivo a ser enviado para ao AG 30 e clique em "OK".

Mensagens no Gateway

Este item exibe todas as mensagens disponíveis no AG 30. Esta mensagem pode ser removida ou baixada para o PC, clicando no botão apropriado.

3.4.9. Reset Geral

Neste caso as configurações de AG 30 voltarão às configurações de fábrica, ou seja, limpará tudo que fora configurado, inclusive o que está rodando e colocará a configuração de fábrica.

4. Configurações de Sistema via CLI

A tabela abaixo mostra como podem ser verificadas as configurações que estão presentes no equipamento.

Tabela 6: Verificação das configurações do sistema

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# show running-config	Exibe a configuração corrente do sistema.
	CPE# show startup-config	Exibe a configuração armazenada na memória permanente.
	CPE# show tech-support	Exibe a configuração corrente do sistema sem as senhas.
	CPE# show versions	Exibe as versões das imagens.
	CPE# show processes	Exibe os processos ativos.
	CPE# show history	Exibe o os últimos comandos executados.
	CPE# show sd	Exibe as estatísticas da memória SD.
	CPE# show clock	Exibe o relógio do sistema.
	CPE# show flash	Exibe as estatísticas da memória flash.
	CPE# show cpu	Exibe as estatísticas da CPU.
	CPE# show memory	Exibe as estatísticas da memória.
	CPE# show privilege	Exibe ao nível de privilégio corrente.
	CPE# show logging	Exibe as informações de log.
	CPE# show network	Exibe as estatísticas de rede e os parâmetros configurados.
	CPE# show interface	Exibe as estatísticas das interfaces de rede e os parâmetros configurados.
	CPE# show arp	Exibe a tabela ARP (Address Resolution Protocol)
	CPE# show ip	Exibe informações relativas a camada IP.
	CPE# show ipv6	Exibe informações relativas ao protocolo IPv6.
	CPE# show ntp	Exibe o NTP (Network Time Protocol).
	CPE# show access-lists	Exibe as listas de acesso configuradas.
	CPE# show route-map	Exibe informações sobre os route maps configurados.
	CPE# show vrrp	Exibe informações sobre o VRRP(Virtual Router Redundancy Protocol)
	CPE# show bfd	Exibe informações sobre o BFD(Bidirectional Forwarding Detection).
	CPE# show link-layer	Exibe informações sobre o protocolos Link Layerr como LLDP, CDP, ...

	CPE# show pbx	Exibe informações sobre o PABX.
	CPE# show licences	Exibe informações sobre as licenças instaladas.
	CPE# show queueing	Exibe informações sobre o as filas (QoS).
	CPE# show voip	Exibe informações sobre o VOIP.
	CPE# show bridge	Exibe informações sobre configurações das bridges
	CPE# show voip sip channels	Mostra o estado dos canais SIP.
	CPE# show voip sip sumary	Mostra confgurações gerais do SIP
	CPE# show voip sip integrated	Mostra configurações dos pontos remotos
	CPE# show voip sip vsp {NUM}	Mostra as configurações do servidor sip definido pelo parâmetro NUM, que pode assumir o valor ‘1’, ‘2’, ‘3’, ‘4’ ou ‘5’.
	CPE# show logging buffer sip	Mostra os logs do SIP.
	CPE# show users	Mostra os usuários que estão logados no momento.
	CPE(config-pbx)#show	O comando “show” mostra as configurações atuais do PABX.

Para escrita de configurações no sistema usam-se os comandos mostrados na tabela abaixo:

Tabela 7: Escrita de configurações no sistema

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE# write	Armazenada as configurações correntes na memória permanente.
4	CPE# copy tftp tftp-server-addrfile-name running-config	Copia as configurações presentes no arquivo indicado por file-name no servidor TFTP indicado por tftp-server-addr para a configuração corrente do sistema.
	CPE# copy running-config tftp tftp-server-addrfile-name	Copia a configuração corrente do sistema para o arquivo indicado por file-name do servidor TFTP indicado por tftp-server-addr.

4.1. Para acesso via CLI

4.1.1. Line VTY

É necessário fazer o primeiro acesso via console e configurar a senha de acesso via SSH, Telnet e Rlogin através do "line vty'", e as senhas e permissões serão usadas sempre que for feito um acesso sem usuário (sem o AAA). Com o AAA ativado as senhas e permissões estarão definidas pelas regras do AAA. Para mais detalhes olhar seção do AAA. O "line vty" possui outras configurações como nível de permissão por acesso, número máximo de terminais permitidos simultâneamente e o uso de access-list para permitir ou bloquear acessos por Iociais diferentes. A senha padrão é *"digistar"*. Abaixo a configuração.

Tabela 8: Programação do line vty

Passo	Comando	Objetivo
1	CPE # configure terminal	Acessa o modo de configuração
2	CPE(config)#line vty	Acessa o nível de configuração Line vty
3	CPE(config-vty)# password {senha}	Configura a senha para acesso via ssh, telnet e Rlogin
4	CPE(config-vty)# max-vty {NUM}	Configura o número máximo de acessos simultâneos. Onde o NUM é de 1 á 10.
5	CPE(config-vty)#level {NUM}	Configura o nível de usuário, NUM é de 1 á 15.
6	CPE(config-vty)#access-class {NUM}	Faz associação a um access-list onde esta configurado o bloqueio ou a liberação de acesso de algum IP. NUM é de 1 á 99.
7	CPE(config-vty)#show	Visualiza as configurações programadas no Line vty.

4.1.2. Line console

Para acesso via console podem ser utilizadas as interfaces Console e Aux0. Por padrão o acesso via console não possui senha, permitindo que todo acesso seja inicialmente permitido. Assim como nas configurações de vty, as senhas e permissões serão usadas sempre que for feito um acesso sem usuário (sem o AAA). Com o AAA ativado as senhas e permissões estarão definidas pelas regras do AAA. Para mais detalhes ver seção do AAA. Abaixo a configuração.

Tabela 9: Programação do line console

Passo	Comando	Objetivo
1	CPE # configure terminal	Acessa o modo de configuração
2	CPE(config)#line console	Acessa o nível de configuração Line console
3	CPE(config-vty)# password {senha}	Configura a senha para acesso via console
5	CPE(config-vty)#level {NUM}	Configura o nível de permissão ao usuário, onde NUM é um valor de 1 a 15.
7	CPE(config-vty)#show	Visualiza as configurações programadas no Line vty.

4.2. Interface

A seguir são apresentados os comandos para configuração das interfaces no CPE. A tabela abaixo descreve como configurar a interface ethernet (10/100/1000) do CPE. O endereço IP e máscara de rede da interface devem estar de acordo com a política de endereços da rede em que a mesma será conectada.

Tabela 10: Configuração de endereço IP na interface ethernet

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber*	Acessa o Modo de Configuraçãoda Interface.
4	CPE(config-*interface*)# ip address {*ip-addrmask* | dhcp}	Atribui o endereço IP e a máscara especificados para a interface ou habilita o cliente DHCP.
5	**Exemplo:** CPE(config)# interface ethernet 1 CPE(config-ethernet0)# ip address 192.168.1.1 255.255.255.0 **Para remover o IP:** CPE(config-ethernet1)# no ip address	Configura a interface ethernet1 com o endereço IP e a máscara especificada.
6	CPE(config-ethernet1)# no shutdown	Ativa a interface ethernet 1. **Importante:** O comando **no shutdown** é responsável por habilitar a interface. É fundamental assegurar-se de que a interface está ativa no momento em que se atribui um endereço para a mesma. Para desabilitar uma interface usa-se **shutdown.**
7	CPE(config-ethernet1)# exit	Retorna ao modo de configuração

4.2.1. Atraso

Com as funcionalidades do comando delay é possível simular algumas propriedades de redes. Pode-se, por exemplo, simular o atraso que um pacote leva para atravessar uma rede qualquer. O atraso é configurável entre os valores 100 e 1000ms, com variância opcional de 50 a 100ms e de acordo ou não com a distribuição probabilística normal, pareto ou pareto-normal.

Tabela 11: Configuração de Atraso

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# *interface ethernet 1*	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# delay *delay [variância]* [distribution {*normal* | *pareto* | *pareto-normal}*] **Exemplo:** CPE(config-ethernet0)# delay 100 50 **Para remover o delay:** CPE(config-ethernet0)# no delay	Configura atraso na interface. **Parâmetros:** **delay:** valor do atraso (ms) **variância:** valor da variância do atraso **normal:** utiliza uma distribuição probabilística normal **pareto:** utiliza uma distribuição probabilística pareto (também conhecida como Bradford) **pareto-normal:** utiliza uma distribuição probabilística pareto-normal O exemplo habilita atraso de 100ms na interface ethernet 1, com variância de 50ms².

4.2.2. DHCP

O DHCP (Dynamic Host Configuration Protocol) (RFC 2131) permite a configuração automática de dispositivos conectados em redes TCP/IP. Os clientes deste protocolo enviam requisições broadcast com o objetivo de obter endereços IP de forma dinâmica, além de informações como gateway padrão e endereço de broadcast.

É possível que o servidor DHCP não esteja no mesmo enlace do cliente e que entre eles exista um roteador que não encaminhe pacotes DHCP. Neste caso é necessário o uso de um elemento intermediário chamado relay DHCP. O relay DHCP é capaz de receber pacotes dos clientes DHCP de sua rede e encaminhar estes pacotes a um servidor pertencente a outra rede.

A tabela a seguir apresenta os comandos para configuração do servidor DHCP:

Tabela 12: Configuração do servidor DHCP

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber*	Acessa o modo de configuração da interface.
4	CPE(config-*interface*)# dhcp-server {broadcast *bcast-addr* | dns *srv-addr [secondary]* | gateway *gw-addr* | lease-time {infinity | *val* {d | h | m} } | mac *mac-addr ip-addr* |mask *mask-add* | on | range *first-addr last-addr*} **Exemplos:** 1) Range de IPs: CPE(config-*interface*)# dhcp-server range 192.168.11.30 192.168.11.60 2) Associação de um endereço MAC com um IP: CPE(config-*interface*)# dhcp-server mac 00:1c:c0:3b:23:b4 192.168.11.68 3) Ligar o servidor DHCP CPE(config-*interface*)# dhcp-server on **Para remover o servidor de DHCP:** CPE(config-*interface*)# no dhcp-server **Para desativar o servidor DHCP:** CPE(config-*interface*)# no dhcp-server on	Acessa o modo de configuração do servidor DHCP. **Opções:** **mask:** Configura uma máscara de rede. (option 1) **gateway:** Configura o endereço do gateway. (option 3) **dns:** Configura o endereço do servidor DNS. Opcionalmente pode ser colocado ainda um ip adicional como secundário. (option 6) **broadcast:** Configura um endereço de broadcast. (option 28) **wins:** Configura o endereço dos servidor wins (option 44) **tftp-server:** Configura o servidor tftp(option 66 para IPs e option 150 para FQDNs) **bootfile-name:** Configura o arquivo que será buscado no servidor tftpboot (option 67) **lease-time:** Especifica o tempo de concessão dos endereços IP como infinito ou em dias, horas ou minutos indicados por *val.* **mac** : Configura a associação de um endereço MAC com um IP específico. **range:** Especifica o range de endereços do DHCP. **on:** Habilita o servidor DHCP *No exemplo 1 define-se uma faixa de endereços a para atribuição via DHCP. Já no exemplo 2 é configurado um IP que será atribuído exclusivamente para o dispositivo com o endereço MAC especificado.*

A seguir são mostrados os passos para configuração do relay DHCP:

Tabela 13: Configuração do relay DHCP

Passo	Comando	Objetivo
1	CPE>enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber*	Acessa o modo de configuração da interface.
4	CPE(config-*interface*)# dhcp-relay *server-addr* **Para remover o DHCP relay:** CPE(config-*interface*)# no dhcp-relay	Configura o servidor de DHCP para o qual serão encaminhadas as requisições recebidas de clientes.

4.2.3. Adição de VLANs

As VLANs (Virtual Local Area Networks) são definidas pelo padrão IEEE 802.1q e consistem em um método para segmentar logicamente as redes locais. Isso é obtido através da inserção de 4 bytes ao cabeçalho do protocolo de encapsulamento de dados. No protocolo Ethernet, os 4 bytes são inseridos entre o endereço de destino e o campo de tamanho e tipo (Type/Length). Entre os campos mais relevantes, estão o identificador do protocolo 802.1q de 16 bits e um identificador da VLAN de 12 bits, que indica a qual VLAN o frame pertence.

A tabela abaixo apresenta os procedimentos para a configuração de VLANs:

Tabela 14: Configuração de VLANs

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config-interface)# exit	Retorna ao modo global de configuração.
4	CPE(config)# interface ethernet intf-number.vlan-id **Exemplo:** CPE (config)# interface ethernet 1.5	Adiciona uma VLAN a interface. O valor do vlan-id deve ser de 1 até 4094. O tag vlan utilizado é 0x8100.
5	CPE(config-ethernet-0.5)# no shutdown	Habilita a sub-interface associada a VLAN. Deste momento em diante pode-se atribuir um endereço IP para a mesma e configurar outras opções, tal como ocorre com qualquer outra interface. Para desabilitar a sub-interface usa-se: **Shutdown**
6	**Para remover uma VLAN** CPE(config)# no interface type intf-number.vlan-id	O comando remove a sub-interface do sistema e todas as configurações que haviam nela.

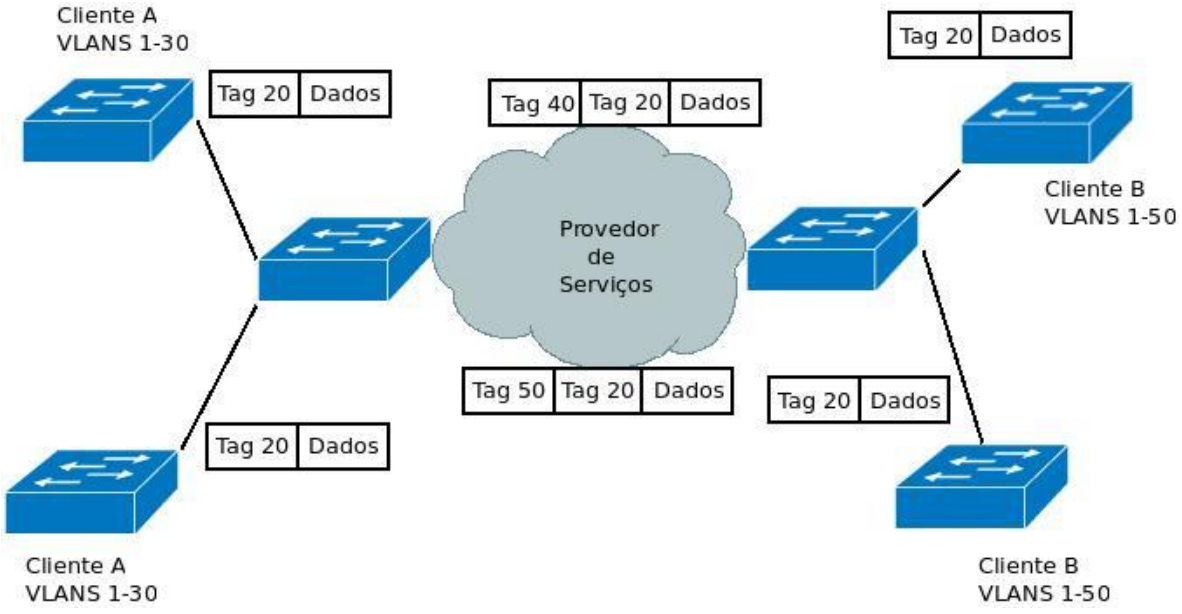
4.2.4. Q in Q: VLAN sobre VLAN

A especificação IEEE 802.1ad, também conhecida como QinQ, estende o padrão IEEE 802.1Q, prevendo o encapsulamento de tags 802.1Q em uma segunda camada de 802.1Q nos roteadores de borda das redes dos provedores de serviços.

O objetivo do QinQ é permitir que quadros de vários clientes possam ser encaminhados (ou tunelados) através da rede do provedor utilizando VLANs de serviço ou S-VLANs. No padrão QinQ, a rede do provedor opera em um espaço de VLANs independente das VLANs utilizadas pelo cliente, mantendo o tráfego de VLANs de diferentes clientes separado.

As VLANS do cliente (Customer VLANs ou C-VLANs) não são utilizadas na tomada de decisões de roteamento no interior da rede do provedor, onde os frames dos clientes são associados as S-VLANs. Assim, na rede do provedor os frames são repassados levando em consideração somente a S-VLAN tag. As C-VLANs são tratatadas como se estivessem blindadas durante essa transmissão. No momento em que o frame deixa a rede do provedor a S-VLAN é removida, sendo dessa forma restaurado o frame original do cliente.

Na figura a seguir, os clientes A e B utilizam a tag 20 em suas VLANs. No entanto, quando os frames de A atravessam a rede do provedor de serviços, é utilizada a VLAN de serviço 40, enquanto que para os frames de B é utilizada a S-VLAN 50.



A tabela abaixo apresenta os procedimentos para configuração de QinQ.

Tabela 15: Configuração de QinQ.

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config-interface)# exit	Retorna ao modo global de configuração.
4	CPE(config)# interface ethernet intf-number.vlan-id.vlan-id2 Exemplo: CPE (config)# interface ethernet 1.5.20	Adiciona uma VLAN sobre VLAN em uma interface. O valor dos vlan-id deve ser de 1 até 4094. Os tags vlan utilizados são 0x8100. Este padrão é conhecido como QinQ.
5	CPE(config-ethernet-1.5.20)# no shutdown	Habilita a sub-interface associada a VLAN. Deste momento em diante pode-se atribuir um endereço IP para a mesma e configurar outras opções, tal como ocorre com qualquer outra interface. Para desabilitar a sub-interface usa-se: Shutdown
6	Para remover uma VLAN CPE(config)# no interface type intf-number.vlan-id.vlan-id2	O comando remove a sub-interface do sistema e todas as configurações que haviam nela.

4.2.5. Outras configurações da interface

A tabela a seguir apresenta configurações de propósito geral das interfaces:

Tabela 16: Configurações gerais da interface

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber*	Acessa o modo de configuração da interface.
4	CPE(config-*interface*)# [no] description *text*	(Opcional) Insere ou remove uma descrição da interface.
5	CPE(config-*interface*)# bandwidth *bw*	(Opcional) Define a largura de banda da interface (em kbps).
6	CPE(config-*interface*)#mtu *mtu*	(Opcional) Define o MTU (*Maximum Transfer Unit*) da interface (em bytes).
7	CPE(config-*interface*)#speed {auto | *speed* {full | half}}	(Opcional) Define a velocidade da interface ou a auto negociação da mesma.

8	CPE(config-*interface*)# [no] multicast	(Opcional) Habilita ou desabilita o tráfego multicast na interface.
9	CPE(config-*interface*)# [no] ip proxy-arp	(Opcional) Habilita ou desabilita o proxy-arp na interface. Com proxy ARP, o roteador pode responder a solicitações ARP em nome de outro dispositivo. Assim, o CPE torna-se responsável por encaminhar os pacotes para seu destino real. O proxy ARP (RFC 1027) permite que um dispositivo em uma subrede alcance outro dispositivo em uma subrede remota sem a necessidade de configurar um default-gateway the need to configure routing or a default gateway.
10	CPE(config-*interface*)# pppoe-client dialer *dialer number*	(Opcional) Configura PPPoE (Point-to-Point Protocol Over Ethernet) na interface (RFC 2516). O parâmetro dialer-number deve ser 0 ou 1. Para remover a configuração do PPPoE usa-se o **no** a frente do comando.
10	CPE (config-interface)# pppoe-client dialer dialer number	(Opcional) Configura PPPoE (Point-to-Point Protocol Over Ethernet) na interface (RFC 2516). O parâmetro dialer-number deve ser 0 ou 1. Para remover a configuração do PPPoE usa-se o **no** a frente do comando.

4.2.6. Internet Protocol Version 6 (IPv6)

4.2.6.1. Considerações Iniciais

O Internet Procotol (IP) é um protocolo da camada de rede, que fornece o serviço de transmissão de datagramas fim-a-fim através de múltiplas redes IP. A versão 4 deste protocolo (IPv4) possui apenas 32 bits para endereços IP, que não fornecem um espaço de endereçamento suficientemente grande para suportar a crescente conexão de novos dispositivos às redes. O Internet Engineering Task Force (IETF) desenvolveu a versão 6 (IPv6) para lidar com este problema, entre outros. O espaço de endereçamento do IPv6 tem uma magnitude muito maior que o do IPv4 ao utilizar 128 bits para endereços IP. Outra característica importante é a eliminação da necessidade de uso de NAPT com o objetivo de aliviar a exaustão de endereços da versão 4. Ele é, portanto, a versão do Internet Protocol que sucede o IPv4.

A versão 6 do protocolo IP, por não suportar interoperabilidade com a versão 4, pode ser considerada um protocolo a parte desta, criando assim, uma nova rede essencialmente paralela à antiga. A comutação de datagramas entre as duas redes requer, a princípio, tradução de protocolos. Contudo, sistemas mais modernos implementam a solução dual-stack, através da qual é possível que a entidade tenha tanto a versão 4 quanto a 6 ao mesmo tempo, possibilitanto a criação de túneis para a interoperabilidade entre as duas redes.

Em resumo, os endereços IPv6 são descritos preferencialmente na forma x:x:x:x:x:x:x:x, em que cada 'x' é a representação hexadecimal dos 16 bits de cada um dos oito pedaços do endereço. Não é necessário escrever os zeros a esquerda dentro de cada bloco 'x' e sequências de zeros podem ser abreviadas por “::”, sendo que não se pode utilizar este recurso mais de uma vez dentro de um mesmo endereço.

Exemplos de representações válidas abaixo:
0123:47:89AB:C:0123:4567:8:CDEF

0000:0000:0000:0012:3456:789A:BCDE:F0123
::12:3456:789A:BCDE:F0123

0123:4567:89AB::

Exemplos de representações inválidas abaixo:
1::2::3

0123:4567:89AB

Para mais informações, assim como explicações sobre a arquitetura de endereços, incluindo endereços reservados, aconselha-se a ler a RFC3513 e consultar http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml para as últimas informações de endereços reservados. Contudo, caso julgue não necessário, a tabela abaixo mostra uma visão resumida e sujeita a mudanças da arquitetura de endereçamento:

Faixa	Propósito
0000::/8	Reservado
0100::/8	Reservado
0200::/7	Reservado
0400::/6	Reservado
0800::/5	Reservado
1000::/4	Reservado
2000::/3	Unicast Global
4000::/3	Reservado
6000::/3	Reservado
8000::/3	Reservado

Faixa	Propósito
A000::/3	Reservado
C000::/3	Reservado
E000::/4	Reservado
F000::/5	Reservado
F800::/6	Reservado
FC00::/7	Unicast Local Único
FE00::/9	Reservado
FE80::/10	Unicast Link Local
FEC0::/10	Reservado
FF00::/8	Multicast

Ressalta-se que o uso de endereços reservados neste equipamento pode causar comportamento inesperado.

4.2.6.1.1. Recursos Suportados

Este produto suporta o protocolo IPv6, definido pela RFC2460 em conjunto com o protocolo ND (Neighbor Discovery), definido pela RFC2461. Também é suportado o modo dual-stack, que permite a coexistência de IPv4 e IPv6. Portanto, todos os recursos de Pv6 podem ser utilizados em conjunto com recursos IPv4.

A versão 6 define diferentes escopos para endereços. Este produto suporta endereços de escopo global,tantos quantos se queiram, e apenas um endereço de escopo link-local por interface. Suporta também a configuração de cliente, relay e servidor DHCP, além das mensagens relacionadas ao protocolo ND, possuindo configurações especiais para a mensagem do tipo Router Advertisement.

Este manual iniciará pela configuração manual de endereços IPv6 e depois seguirá para os tópicos de autoconfiguração.

4.2.6.2. Configuração de Endereços IPv6

Esta seção trata da atribuição de endereços às interfaces. Normalmente, uma interface com IPv6 possui 2 endereços, um de escopo link-local e outro de escopo global. O primeiro é automaticamente gerado a partir do endereço MAC da camada de enlace, mas pode ser configurado manualmente ou removido. O segundo pode ser configurado manualmente, gerado a partir do MAC ou autoconfigurado. Trataremos cada caso nas próximas seções.

4.2.6.2.1. Configuração de endereço de escopo Link-Local

Ao ligar a interface, um endereço IPv6 de escopo link-local é automaticamente gerado a partir do endereço MAC. Caso queira-se modificar este endereço, pode-se utilizar os comandos listado na tabela abaixo. Para removê-lo, use a forma no do comando.

Tabela 17: Configuração de Endereço Link-Local

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 address link-local *address* **Exemplo:** CPE(config-ethernet0)# ipv6 address link-local address fe80::1	Configura a interface com endereço *address* link-local. **Parâmetros:** *address*: endereço IPv6 link-local (FE80:X::X:X) O exemplo configura o CPE com o endereço de escopo link-local fe80::1 na interface ethernet 1.

4.2.6.2.2. Configuração manual de endereço de escopo Global

Utilizando-se os comandos da tabela abaixo, é possível configurar endereços de escopo global nas interfaces. Para remover cada endereço deve-se utilizar a forma no do comando. É possível que se tenha tantos endereços IPv6 deste escopo quanto se queira, utilizando os comandos abaixo o mesmo número de vezes.

Tabela 18: Configuração de Endereço Global

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 address *address* **Exemplo:** CPE(config-ethernet0)# ipv6 address 1234::abcd/3	Configura a interface com endereço *address* global. **Parâmetros:** *address:* endereço IPv6 de escopo global O exemplo configura o CPE com o endereço 1234::abcd na interface ethernet 1.

4.2.6.2.3. Configuração de endereço de escopo Global com o método eui-64

Utilizando-se os comandos da tabela abaixo, é possível configurar endereços de acordo com o método EUI-64 e de escopo global nas interfaces. Para remover cada endereço deve-se utilizar a forma no do comando.

Tabela 19: Configuração de Endereço com EUI-64

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 address *address eui-64* **Exemplo:** CPE(config-ethernet0)# ipv6 address 5555::/64 eui-64	Configura a interface com o endereço composto pelo prefixo *prefix* e o sufixo gerado de acordo com o método eui-64. Escopo Global. **Parâmetros:** *prefix:* endereço IPv6 de escopo global O exemplo configura o CPE com o endereço gerado pelo método eui-64 de prefixo 5555::/64 na interface ethernet 1.

4.2.6.2.4. Autoconfiguração

Este produto suporta a autoconfiguração de endereços IPv6 na interface. Este modo configura um endereço de escopo link-local baseando-se no endereço MAC da camada abaixo e utiliza cliente DHCP para obter um endereço global. Evidentemente, é necessário que se tenha um servidor DHCP para IPv6 presente na rede. Para habilitar, siga os comandos abaixo.

Tabela 20: Autoconfiguração

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 address autoconfig **Exemplo:** CPE(config-ethernet0)# ipv6 address autoconfig	Habilita autoconfiguração na interface. O exemplo configura o CPE com autoconfiguração de endereço IPv6 na interface.

4.2.6.2.5. Obtenção de endereço por DHCP

Obtém-se um endereço global através do uso de um cliente DHCP. É necessário que se tenha um servidor DHCP para IPv6 presente na rede. Para habilitar, siga os comandos abaixo.

Tabela 21: Configuração de Cliente DHCP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 address dhcp [rapid-commit][no-address] **Exemplo:** CPE(config-ethernet0)# ipv6 address dhcp	Configura a interface com Cliente DHCP para endereço IPv6. **Parâmetros:** rapid-commit: habilita *rapid-commit* para obtenção do endereço. No-address: desabilita a obtenção do endereço, assumindo somente os outros parâmetros. O exemplo configura o CPE com Cliente DHCP para IPv6 na interface ethernet0.

4.2.6.3. Configuração Router Advertisements (RA)

As mensagens do tipo RA são geradas por roteadores que suportam o protocolo ND. Estas mensagens estão descritas na seção 4.2 da RFC deste protocolo (RFC2461). Neste item são mostradas as configurações possíveis relacionadas a este tipo de mensagem. Hosts utilizam estas mensagens para se autoconfigurar. Roteadores ignoram estas mensagens.

4.2.6.3.1. Habilitação

Por padrão, o CPE não envia mensagens RA. Para habilitar, utilize o comando abaixo:

Tabela 22: Habilitar envio de mensagens Router Advertisement

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** *CPE (config)# interface ethernet 1*	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# no ipv6 nd ra supress	Configura o CPE para enviar mensagens RA na interface.

4.2.6.3.2. Prefixos

Em cada mensagem RA, são incluídos os prefixos que se deseja informar aos hosts da rede. Os hosts utilizam estes prefixos para gerarem endereços próprios IPv6 através do método EUI-64 (autoconfiguração). Por padrão, os prefixos de endereços configurados manualmente são incluídos nas mensagens, mas podem ser removidos através da forma no do comando.

Cada prefixo possui configurações adicionais: um tempo de validade (valid-lifetime), um tempo preferencial de uso (preferred-lifetime) e as seguintes flags de configuração:

1) no-autoconfig: não utilizar o prefixo para autoconfiguração (não gerar endereço com eui-64)
2) no-onlink: priopriedade on-link ou off-link do prefixo.
3) no-rtr-address: envia endereço da interface e não o prefixo. Mobile IPv6.

Para adicionar novos prefixos ou modificar parâmetros de prefixos existentes, utilize os comandos listados abaixo:

Tabela 23: Configuração de Prefixo

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)*# interface ethernet 1*	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd {prefix *prefix* / default { *valid-lifetime* / infinite | no-advertive} [*preferred-lifetime* | infinite] [no-autoconfig] [no-onlink] [no-rtr-address] } **Exemplo:** CPE(config-ethernet0)#ipv6 nd prefix 2222::/64 infinite infinite	Configura o CPE para enviar mensagens RA de tal prefixo na interface, com as opções configuradas. **Parâmetros:** *prefix:* prefixo que se deseja adicionar ou modificar parâmetros. *Default* modifica as configurações de todos prefixo. *valid-lifetime*: número de segundos que um prefixo é valido (ou infinito) *preferred-lifetime*: número de segundos que se deseja que o prefixo seja utilizado (ou infinito) *no-autoconfig:* habilita a flag *no-onlink:* habilita a flag *no-rtr-address:* habilita a flag O exemplo adiciona um prefixo 2222::/64 com tempos infinitos aos RAs na interface ethernet 1.

Configuração de RA Hop-Limit

Para especificar manualmente o número de saltos (hops) máximos que uma mensagem RA pode dar, utilize o comando abaixo.

Tabela 24: Configuração de RA Hop-Limit

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd ra hop-limit {*valor* | unspecified} **Exemplo:** CPE(config-ethernet1)#ipv6 nd ra hop-limit 16	Configura o valor de Hop-Limit das mensagens RA. **Parâmetros:** *valor*: número de saltos. O valor 0 significa não especificado. *Unspecifed*: Não define numero de saltos. O exemplo configura os RAs enviados com *hop-limit* 16 na interface ethernet 1.

Configuração de RA Interval

Para especificar manualmente o espaço de tempo entre dois RAs, utilize os comandos listados na tabela abaixo.

Tabela 25: Configuração de RA Interval

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd ra interval *valor* **Exemplo:** CPE(config-ethernet0)#ipv6 nd ra interval 60	Configura o intervalo entre uma mensagem RA e outra. **Parâmetros:** *valor*: segundos entre um RA e outro. O exemplo configura os RAs com intervalo de 60 segundos na interface ethernet 1.

Configuração de RA MTU

Especifica manualmente o valor da opção MTU nas mensagens RA. Este campo é útil para que os hosts todos se configurem com o mesmo MTU.

Tabela 26: Configuração de RA MTU

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd ra mtu *valor* **Exemplo:** CPE(config-ethernet1)# ipv6 nd ra mtu *1400*	Configura o valor da opção MTU das mensagens RA. **Parâmetros:** *valor*: número de bytes de MTU O exemplo configura os RAs enviados com opção MTU 1400 bytes na interface ethernet 1.

4.2.6.3.3. Opção Advertisement Interval

Em cada mensagem RA, pode ser enviando um campo opcional sinalizando para os receptores de quanto em quanto tempo eles devem esperar mensagens RA. Este parâmetro é apenas informativo, não confundir com o intervalo de fato entre cada mensagem RA. Utilizado por Mobile IPv6. Para configurar, utilize os comandos da tabela abaixo.

Tabela 27: Flag Advertisement Interval

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	/6 nd *advertisement-interval*	Habilita o envio de Advertisement Interval.

4.2.7.1.1. Opção Managed Configuration

Esta opção habilita uma flag nas mensagens RA solicitando os receptores para que utilizem DHCP para obter seus endereços. Para configurar, utilize os comandos da tabela abaixo.

Tabela 28: Flag Managed Configuration

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-ethernet1)# ipv6 nd *managed-config-flag*	Habilita o envio da flag managed-config na interface ethernet 1.

4.2.7.1.2. Opção Other Configuration

Esta opção habilita uma flag nas mensagens RA solicitando os receptores para que utilizem DHCP para obter informações sobre configuração, exceto endereço (DHCP stateless). Para configurar, utilize os comandos da tabela abaixo.

Tabela 29: Flag Other Configuration

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-ethernet1)# ipv6 nd other-*config-flag*	Habilita o envio da flag other-config na interface ethernet 1.

4.2.7.1.3. Opção Neighbor Solicitation (NS) Interval

Esta opção informa aos receptores, na mensagem RA, o tempo de retransmissão entre cada mensagem Router Solicitation (RS). Para configurar, utilize os comandos da tabela abaixo.

Tabela 30: Configuração de NS Interval

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd ns-interval *valor* **Exemplo:** CPE(config-ethernet1)#ipv6 nd ns 10000	Configura o valor de NS Interval nas mensagens RA. **Parâmetros:** *valor*: tempo em milisegundos. O exemplo configura para 10000ms na interface ethernet 1.

4.2.7.1.4. Opção Reachable Time

Esta opção informa aos receptores, na mensagem RA, o tempo de alcance na rede (reachable-time). Para configurar, utilize os comandos da tabela abaixo.

Tabela 31: Configuração de Reachable Time

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd reachable-time *valor* **Exemplo:** CPE(config-ethernet1)#ipv6 nd reachable-time 30000	Configura o valor de *Reachable Time* nas mensagens RA. **Parâmetros:** *valor*: tempo em milisegundos. O exemplo configura para 30000ms na interface ethernet 1.

4.2.7.1.5. Opção Router Preference

Esta opção modifica a preferência das mensagens RA enviadas por este CPE. O valor padrão é medium. Para configurar, utilize os comandos da tabela abaixo.

Tabela 32: Configuração Router Preference

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 nd router-preferece { high | medium | low } **Exemplo:** CPE(config-ethernet1)#ipv6 nd router-preference high	Configura a preferência deste CPE. **Parâmetros:** high: Envio mensagens RA como CPE preferencial medium: Opção default low: Envio mensagens RA como CPE menos preferencial O exemplo configura para alta preferência na interface ethernet1.

4.2.7.2. Configuração de Servidor DHCP

A configuração de servidor DHCP para IPv6 é feita por interface. É necessária a configuração de um intervalo de endereços para que o servidor de fato inicie, mesmo que seja utilizado o modo stateless. Para configurar, utilize os comandos listados abaixo:

Tabela 33: Configuração Servidor DHCP IPv6

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 dhcp-server **Exemplo:** CPE(config-ethernet0)# ipv6 dhcp-server	Acessa o modo de configuração do servidor DHCP para IPv6 da interface.
5	CPE(config-interface-dhcp6)# range *low high* ***Exemplo:*** CPE(config-ethernet1-dhcp6)#range 5000::1 5000::ffff	Configura o intervalo de endereços DHCP. **Parâmetros:** *low:* primeiro endereço da faixa *high:* último endereço da faixa O exemplo configura o servidor DHCP para distruibuir endereços entre 5000::1 e 5000::ffff
6	CPE(config-interface-dhcp6)#dns *primary* [*secondary*] **Exemplo:** CPE(config-ethernet1-dhcp6)# dns 5023::4	(OPCIONAL) Configura o servidor DHCP para fornecer configuração de DNS. **Parâmetros:** *primary:* IP do servidor dns primário *secondary:* IP do servidor dns secundário O exemplo configura o servidor para incluir a configuração de dns primário 5023::4.

7	CPE(config-interface-dhcp6)# domain-name *domain* **Exemplo:** CPE(config-ethernet1-dhcp6)#domain-name digistar	(OPCIONAL) Configura o servidor DHCP para fornecer domínio. **Parâmetros:** *domain:* nome do domínio O exemplo configura o servidor para incluir a configuração de nome de domínio digistar
8	CPE(config-interface-dhcp6)#preferred-life-time *life* **Exemplo:** CPE(config-ethernet1-dhcp6)#preferred-life-time 5000	(OPCIONAL) Especifica o tempo de vida preferencial de cada endereço. **Parâmetros:** *life:* tempo em segundos O exemplo configura o servidor para distribuir endereços com um tempo de vida preferencial de 5000 segundos.
9	CPE(config-interface-dhcp6)#rapid-commit	(OPCIONAL) Habilita Rapid-Commit
10	CPE(config-interface-dhcp6)#server-preference *value* **Exemplo:** *CPE(config-ethernet0-dhcp6)#server-preference 100*	(OPCIONAL) Configura a preferência do servidor DHCP. Quanto maior o valor, maior a preferência. **Parâmetros:** *value:* valor da preferência (0 a 255) O exemplo configura o servidor com preferência 100.
11	CPE(config-interface-dhcp6)#use-ra-prefix	(OPCIONAL) Configura o servidor para sinalizar aos clientes que estes devem utilizar RAs para configurarem seus endereços.
12	CPE(config-interface-dhcp6)#valid-life-time *life* **Exemplo:** CPE(config-ethernet1-dhcp6)#valid-life-time 10000	(OPCIONAL) Especifica o tempo de validade máxima para cada endereço. **Parâmetros:** *life:* tempo em segundos O exemplo configura o servidor para distribuir endereços com um tempo validade de 10000 segundos.

4.2.7.3. Configuração de Relay DHCP

Para configurar DHCP Relay para IPv6 na interface, utilize os comandos listados abaixo:

Tabela 34: Configuração Relay DHCP IPv6

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *typenumber* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ipv6 dhcp-relay *address* **Exemplo:** CPE(config-ethernet1)#ipv6 dhcp-relay 1234::abcd	Configura relay na interface. **Parâmetros:** *address*: endereço do servidor DHCP ou de outro relay O exemplo configura a função relay na interface ethernet0 para o IP 1234::abcd

4.2.7.4. Configuração de Cliente DHCP sem obtenção de endereço

É possível configurar um cliente DHCP em uma interface para que ele obtenha todas configurações da rede, exceto um endereço IP (Stateless). O endereço IP pode ser obtido por outros mecanismos, como mensagens RA. Para habilitar, siga os comandos abaixo.

Tabela 35: Configuração Cliente DHCP Stateless

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface typenumber **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)# ipv6 address dhcp no-address **Exemplo:** CPE(config-ethernet0)# ipv6 address dhcp no-address	Configura cliente sem obtenção de endereço na interface. O exemplo configura a interface ethernet 0 para obtenção das configurações de rede via DHCP.

4.3. DNS

O DNS (Domain Name System) (RFC 1034) (RFC 1035) é um recurso utilizado em redes TCP/IP que permite acessar computadores através de nomes amigáveis, sem que o usuário ou sem que o próprio computador tenha conhecimento de seu endereço IP. Os serviços de DNS da internet encontram-se distribuídos em bancos de dados de servidores de todo o mundo. Estes bancos de dados podem indicar o endereço IP associado a um nome de um site.

A tabela mostra como configurar um servidor de nomes:

Tabela 36: Configuração de um servidor de nomes

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] ip *[vrf vrf-name]* name-server *ip [priority <1-10>]* **Exemplo:** CPE (config)# ip name-server 8.8.8.8	Configura ou remove um servidor de nomes.

Comandos relacionados

CPE (config)# [no] ip dns server	Habilita ou desabilita a criação de uma tabela local com todos os domínios já resolvidos para acelerar o processo de resolução.
CPE (config)# [no] ip domain lookup	Habilita ou desabilita a funcionalidade que permite obter o endereço IP a partir do endereço do domínio.

4.4. DNS Dinâmico

O DNS dinâmico (RFC 2136) é um modo de associar um FQDN (Fully Qualified Domain Name) a um endereço IP dinâmico. Devido a quantidade limitada de endereços IP na Internet, quando uma máquina é desconectada, o endereço IP associado a ela é realocado. O DNS dinâmico permite que um computador seja acessado mesmo com a ocorrência de mudanças constantes no endereço IP.

Podem ser inseridos no sistema manualmente (configuração abaixo) ou provenientes de servidores de DHCP client e PPPoE client. Para saber quais DNS realmente ficaram no sistema e qual o melhor servidor, podemos definir uma prioridade para cada name-server.

Para o correto funcionamento todas as VRFs devem ter seus name-servers configurados.

Abaixo constam os procedimentos para adição de um DNS dinâmico:

Tabela 37: Configuração de DNS dinâmico

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] ddns LABEL	Define ou remove um label para a configuração de DDNS.
4	CPE (config-ddns-label)# {backup-mx FQDN | domain FQDN | login login | natt | provider provider | type {dinamic hours | static} | wildcards | shutdown}	**Opções:** **backup-mx:** Configura o uso de um backup MX . **domain:** Configura o nome do domínio . **login:** Configura o login para o serviço DDNS. **natt:** Configura o uso de NATT para a obtenção de endereços IP públicos. **provider:** Configura o provedor DDNS. **shutdown**: Desabilita a conta. **type:** Define o tipo de serviço DDNS (estático ou dinâmico. **Wildcards:** Habilita o uso de DDNS wildcard .
5	CPE (config-ddns-label)# exit	Retorna ao modo de configuração.

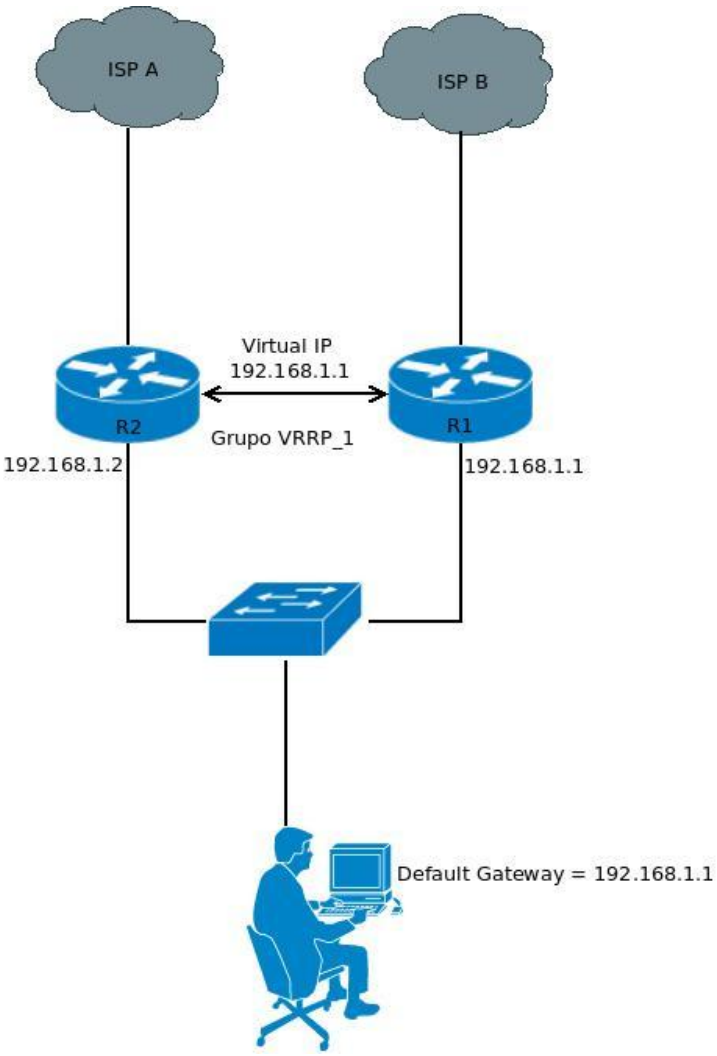
4.5. Virtual Router Redundancy Protocol – VRRP

O Virtual Router Redundancy Protocol (VRRP) (RFC 5798) é um protocolo que utiliza eleição para chavear o tráfego de um roteador para outro, em caso de queda no link, ou do próprio roteador. Um roteador VRRP é configurado para executar o protocolo VRRP juntamente com um ou mais roteadores conectados a uma LAN. Um roteador deve ser configurado como mestre e os demais como backups para suprir as eventuais falhas do mestre.

Para minimizar o tráfego de rede, somente o mestre de cada roteador virtual envia periódicamente anúncios VRRP. O roteador virtual é uma abstração que atua para os demais dispositivos conectados a LAN como defalult gateway.

Um roteador que é backup não vai tentar assumir o papel de master a menos que tenha maior prioridade. Também é possível proibir administrativamente as tentativas de preempção. Porém, um roteador VRRP sempre irá se tornar mestre se o endereço do roteador virtual estiver associado a uma de suas interfaces. Se o mestre fica indisponível, então o backup de maior prioridade fará a transição para estado mestre, após um pequeno atraso, passando a enviar anúncios VRRP e a responder pelo IP do roteador virtual. Quando o roteador que era mestre originalmente voltar a atividade, este assumirá novamente o seu papel e passará a enviar os anúncios VRRP.

Se existirem diversos roteadores VRRP em um grupo e o mestre falhar, assumirá como novo mestre aquele que tiver maior prioridade. A figura a seguir mostra uma rede com VRRP.



O roteador R1 tem em sua interface o endereço IP virtual do grupo VRRP_1 (no caso, 192.168.1.1). Por este motivo, ele é o mestre. Este endereço é conhecido pelos hosts da rede como sendo o do default gateway. Em caso de falha do roteador mestre R1, R2 assumirá como mestre e passará a responder pelo IP 192.168.1.1, fazendo com que a transição ocorra de forma transparente para o usuário. A tabela a seguir apresenta os comandos para configuração do VRRP.

Tabela 38: Configuração do VRRP

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface *type number*	Acessa o Modo de Configuração da Interface.
4	CPE(config-*interface*)# ip address 192.168.1.1 255.255.255.0	Atribui um endereço IP a interface.
5	CPE(config-*interface*)# vrrp *group* authentication {ah *string* | text *string*}	(Opcional) Para VRRP com implementação antiga(RFC 2338) exite um método de autenticação por texto simples ou por autenticação de cabeçalho Ah – autenticação de cabeçalho Text – texto simples
6	CPE(config-*interface*)# vrrp *group* description *text* **Exemplo:** CPE(config-ethernet1)# vrrp 1 description VRRP_1	Associa uma descrição textual a um grupo VRRP. Os valores possíveis para o grupo são 1-255. Para remover a descrição usa-se: **no vrrp *group* description**
7	CPE(config-*interface*)# vrrp *group* priority *level* **Exemplo:** CPE(config-ethernet1)# vrrp *1* priority *120*	Define a prioridade do CPE dentro de um grupo VRRP. O valor *default* para a prioridade é 100. Para remover a prioridade usa-se: **no vrrp *group* priority**
8	CPE(config-*interface*)# [no] vrrp *grupo* preempt [delay minimum *seconds*] **Exemplo:** CPE(config-ethernet1)# vrrp *1* preempt delay minimum 200	Configura o CPE para assumir como master em um grupo VRRP se ele possui prioridade maior do que o master atual. O valor *default* para o *delay* é de 0 segundos e o roteador que possui o IP virtual configurado em uma de suas interfaces sempre que estiver ativo assumirá como mestre, ainda que a preempção esteja desabilitada (a mesma é habilitada por *default*). Para remover esta configuração usa-se o **no** a frente do comando.
9	CPE (config-*interface*)# vrrp *group* timers advertise [msec] *interval* **Exemplo:** CPE (config-ethernet1)# vrrp *120* timers advertise 100	Configura o intervalo entre os anúncios sucessivos enviados pelo roteador *master* de um grupo VRRP. O intervalo é dado em segundos exceto quando *msec* é especificado na configuração. O intervalo *default* é de 1 segundo. Dentro de um grupo VRRP todos os roteadores devem utilizar os mesmos intervalos. Para remover o intervalo configurado usa-se: **no vrrp *group*timers advertise**

10	CPE (config-*interface*)# [no] vrrp group ip *ip-address [secondary]* ***Exemplo:*** *CPE (config-ethernet1)# vrrp 1 ip 192.168.1.1*	Habilita o VRRP na interface. Além do endereço IP primário, pode ser usado ainda um IP secundário. Todos os roteadores de um grupo VRRP devem ser configurados com o mesmo endereço primário e, quando for o caso, secundário. Se o endereço IP virtual configurado aqui for o mesmo da interface do roteador, este assume como master e passa a ter prioridade 255 (ainda que outro valor tenha sido configurado anteriormente). Para desabilitar o VRRP na interface usa-se o **no** a frente do comando.
11	CPE (config-if-ethernet1)# exit	Retorna ao modo de configuração

4.5.1. Adição de VRRP Track

O CPE permite a configuração de objetos para serem monitorados e de acordo com o estado dos mesmos, modificar a prioridade do roteador dentro de um grupo VRRP. As configurações correspondentes são apresentadas a seguir.

Tabela 39: Monitoração de objetos no VRRP

Passo	Comando	Objetivos
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# track object_value interface type number line-protocol CPE (config)# track objet_value ip route route/mask reachability CPE (config)# track timer ip route time_seconds **Exemplo 1:** CPE (config)# track 2 interface ethernet 1 line-protocol **Exemplo 2:** CPE (config)# track 2 ip route 192.168.10.0/24 reachability	Configura uma interface para ter o seu estado monitorado. As mudanças no estado influenciam na prioridade do roteador dentro de um grupo VRRP. No exemplo 1, são configurados a interface que será verificada quanto ao seu estado (UP/DOWN) e o objeto correspondente a ser utilizado com o comando vrrp track (a ser aplicado na interface onde o VRRP está habilitado). No exemplo 2, o comando track objeto ip route permite que seja verificada se uma determinada rota pode ser alcançada através de alguma interface. Para remover o VRRP track na interface usa-se o **no** a frente do comando.
4	CPE(config-ethernet1)# vrrp group track object_value [decrement decrement_value] **Exemplo:** CPE(config-ethernet0)# vrrp 1 track 2	Configura a monitoração de um objeto e decrementa de 20 a prioridade do roteador se a interface monitorada está DOWN ou se a rota especificada está inalcançável, de acordo com a etapa anterior. Para remover o VRRP track na interface usa-se: **no vrrp** group **track**

4.6. Bidirectional Forwarding Detection – BFD

(recurso habilitado por licença)

O Bidirectional Forwarding Detection (BFD) (RFC 5880) (RFC 5883) é um protocolo que provê detecção rápida de falhas no caminho entre roteadores adjacentes. O BFD foi pensado para atuar em conjunto com qualquer protocolo de roteamento, encapsulamento ou meio de transmissão, consistindo em um método de detecção de falhas mais rápido do que as mensagens do tipo hello dos protocolos de roteamento.

O BFD é habilitado nas interfaces e nos protocolos de roteamento, devendo ser configurado nos dois roteadores adjacentes, a fim de que possa ser estabelecida uma sessão BFD entre os mesmos, na qual são inicialmente negociados os timers. Concluída esta negociação, os roteadores passam a trocar pacotes de controle BFD respeitando o intervalo negociado. Esta troca de mensagens ocorre de modo similar ao que acontece no envio de mensagens hello nos protocolos de roteamento, porém em intervalos de tempo muito menores. Na implementação presente nos equipamentos da Digistar os pacotes BFD são encapsulados em UDP (User Datagram Protocol).

Os pacotes de controle BFD contêm entre outras informações o estado da seção do sistema local (que pode ser init, up, down ou administratively down)., o local discriminator e o remote discriminator (que identificam a sessão BFD no sistema local e remoto, respectivamente) e o local diagnostic (que é um código que especifica a razão da mudança mais recente no estado da sessão no sistema local).

Quando o BFD detecta a ocorrência de uma falha, a realização de uma ação adequada fica sob a responsabilidade do protocolo de roteamento.

A figura abaixo mostra dois roteadores executando OSPF ou BGP e utilizando BFD para detecção de falhas. No momento em que o OSPF ou o BGP estabelecem uma relação de vizinhança (1), eles notificam o processo BFD para iniciar uma sessão com o equipamento vizinho (2).

Já na figura a seguir é mostrado o momento em que ocorre uma falha na rede. A sessão BFD entra em estado down (3)e o processo BFD notifica o OSPF ou o BGP sobre a falha (4). Neste momento, o OSPF ou o BGP encerram a respectiva sessão e se existe uma rota alternativa àquela que se tornou indisponível, passam a utilizá-la.

Os procedimentos para configuração do BFD nas interfaces estão detalhados na tabela abaixo:

Tabela 40: Configuração de BFD nas interfaces

Passo	Comando	Objetivos
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number	Acessa o modo de configuração da interface.
4	CPE(config-interface)# bfd interval value_min_rx value_multiplier interval-multiplier **Exemplo:** CPE(config-interface)# bfd interval 100 min_rx 100 multiplier 5	(Opcional) Habilita o BFD na interface. **Parâmetros:** **interval:** É o intervalo mínimo entre os pacotes de controle BFD transmitidos que o sistema local deseja adotar no momento. **min_rx:** É o intervalo mínimo entre os pacotes de controle BFD recebidos que o sistema local deseja adotar no momento. **multiplier:** É o multiplicador para o tempo de detecção de falhas desejado pelo sistema local. O intervalo para envio de pacotes negociado entre os roteadores multiplicado por esta variável fornece o tempo para detecção de falhas. No exemplo são configurados intervalos de 100 ms para envio e recebimento de pacotes BFD. O tempo que o sistema deve permanecer sem receber pacotes para considerar que ocorreu falha é de **5*100 ms = 500 ms**.

4.6.1. Configuração do BFD nos protocolos de roteamento

Para que a sessão BFD possa ser estabelecida e os pacotes de controle possam ser trocados entre os roteadores adjacentes, é necessário configurar o BFD nos protocolos de roteamento. Osprocedimentos para configuração encontram-se nas seções dedicadas a estes protocolos–Configuração do BFD no OSPF e Configuração do BFD no BGP.

4.7. Permissões

Esta seção apresenta os comandos para configuração de listas de controle de acesso (Acess Control Lists – ACLs) e regras para tradução de endereços (Network Address Translation – NAT).

4.7.1. Access Control Lists - ACLs

O AG 30 Plus implementa dois tipos de Access Control Lists – as listas padrões(standard ACLs) e as listas estendidas (extended ACLs). Em ambos os casos é utilizado o conceito de negar todo o tráfego e permitir somente o que for informado. Deste modo, todas as ACLs terminam com um **deny any** implícito. As ACLs padrão são numeradas de 1 a 99 e de 1300 a 1999, enquanto que as estendidas são numeradas de 100 a 199 e de 2000 a 2699. O que diferencia estes dois tipos são os procedimentos seguidos na inspeção do pacote IP – listas padrões verificam somente o endereço de origem no cabeçalho IP, enquanto que as listas estendidas observam o endereço IP de origem e destino e o cabeçalho de segmentos encapsulados no pacote IP (RFC 3232) (RFC 1918) (RFC 1858).

4.7.1.1. Adição de ACLs

As ACLs podem ser aplicadas as interfaces e em outros contextos, como por exemplo, para controlar o anúncio de rotas. Durante a configuração de ACLs é necessário fazer uso de máscaras wild card. O conceito de wild card é detalhado a seguir:

Máscara de wild card

Essa máscara é um valor de 32 bits e informa ao roteador quais bits que do endereço IP devem ser ignorados. Uma máscara wildcard é muito similar a uma máscara de sub-rede, porém com a lógica invertida: Um binário 1 na máscara wildcard significa “bit irrelevante”, enquanto que o bit 0 na máscara wildcard distingue os bits importantes.

Exemplo:
Considere o endereço de rede **172.2.1.0** com wild card **0.0.0.255.**

Transformando os octetos do wild card em binários, temos:

0.0.0.255 = 00000000.00000000.00000000.11111111

No último octeto temos todos os bits em 1, indicando que a parcela correspondente do endereço IP deve ser ignorada. Os bits a serem ignorados podem constar em qualquer parte do endereço IP, ao contrário do que acontece na máscara de sub-rede.

De posse da máscara de sub-rede, pode ser usado o seguinte procedimento para obtenção do wild card:

Subtrai-se cada octeto da máscara de sub-rede (em formato decimal) de 255, conforme mostra o exemplo abaixo:

- máscara de rede: 255.255.224.0
- máscara wildcard: ???.???.???.???
- primeiro octeto → 255- 255 - máscara de sub-rede = 255 - 255 = **0**
- terceiro octeto → 255 - máscara de sub-rede = 255 - 224 = **31**
- quarto octeto → 255 - máscara de sub-rede = 255 - 0 = **255**
- máscara wild card: **0.0.31.255**

A mesma lógica se aplica para endereços IPv6 e MAC.

A seguir são detalhados os procedimentos necessários para a configuração de ACLs:

Tabela 41: Configuração e aplicação de listas de acesso padrão

Passo	Comando	Objetivos
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# access-list *access-list-number* {permit | deny | remark *remark_LINE*| resequence *start-number increment-value* | seq *seq-number*} {host *host-ip* | source *source source-wildcard*| any} **Exemplo:** CPE(config)#access-list 1 deny 192.168.100.00.0.0.255 CPE(config)#access-list 1 deny 192.168.99.00.0.0.255 CPE(config)#access-list 1 permit any	Configura uma access-list padrão **Parâmetros e opções:** **access-list-number:**Número da lista, de 1 até 99 e de 1300 até 1999. **permit / deny:** Ação a ser realizada quando o pacote atende aos requisitos especificados na ACL – permite ou nega. **host:** Um endereço de máquina específico indicado em *host-ip.* **source:** Um endereço de rede / máscara específicos indicados em *source source-wildcard.* **any:** Indica que a ACL é aplicável a qualquer fonte. Esta configuração faz com que os pacotes originados nas redes especificadas sejam rejeitados pelo roteador. As ACLs são analisadas de cima para baixo e o processamento das mesmas é encerrado no momento em que o pacote que é verificado atende ao critério especificado em uma linha. Ao final de uma lista tem-se implícita a linha ***deny any***. Neste exemplo, devido ao uso da palavra-chave ***deny*** serão processados pelo roteador somente os pacotes que ***não*** atenderem aos requisitos especificados. Se a linha ***access-list 1 permit any*** não estivesse presente, todo o tráfego seria rejeitado. Em outras palavras, uma lista que tem ***deny*** em todas as linhas faz com que todo o tráfego seja rejeitado. Após definir uma access-list é necessário aplicar a mesma em uma interface, conforme é mostrado no passo 4 (ACLs não aplicadas não tem nenhum efeito). Para remover uma ACL usa-se: **no access-list *access-list-number*** **no access-list {*access-list-number* | sequence-numbers}**

4	CPE(config)# interface type number	Entra no modo de configuração da interface.
5	CPE(config-interface)# ip access-group access-list-number {in | out} **Exemplo:** CPE(config-ethernet0)# ip access-group 1 in.	Aplica a access-list em uma interface. No exemplo é aplicada a ACL definida no passo 4 na interface ethernet 0 no sentido de entrada. Para remover uma ACL da interface usa-se: **no ip access-group access-list-number {in | out}**
6	CPE (config-ethernet0)# exit	Sai do modo de configuração da interface.

Para as ACLs estendidas os passos 3 e 4 constam abaixo:

Tabela 42: Configuração e aplicação de listas de acesso estendidas

Passo	Comando	Objetivos
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	IP, AH, EIGRP, ESP, GRE, IPIP, OSPF, PIM CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE | resequence start-number increment-value | seq seq-number} protocol {host host-ip | source source source-wildcard | any} {host host-ip | destination destination-wildcard | any} [precedence precedence] [tos tos][log] [dscp dscp_mark][fragments][time-rangeWORD] 2) ICMP CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE | resequence start-number increment-value | seq seq-number} icmp {host host-ip | source source source-wildcard | any} {host host-ip | destination destination-wildcard | any} [**icmp-type [icmp-message]** [precedence precedence] [tos tos][log] [dscp dscp_mark] [fragments] [time-range WORD] 3) TCP CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE| resequence start-number increment-value | seq seq-number} tcp {host host-ip | source source source-wildcard | any} [operator [port]] {host host-ip | destination destination-wildcard | any} [operator [port]] [established] [precedence precedence] [tos tos][log][dscp dscp_mark] [fragments] [time-range WORD] [ack | fin | new | psh | rst | syn | urg]	Configura uma access-list estendida. Neste caso, a numeração das listas é de 100 até 199 e de 2000 até 2699. **Parâmetros e opções:** **established:**Somente para o protocolo TCP. A aplicação da ACL ocorre quando o datagrama TCP tem os bits ACK ou RST setados, ou seja, para conexões já estabelecidas. **precedence:** É possível filtrar pacotes de acordo com o nível de precedência (de 0 até 7). **tos:** É possível filtrar pacotes de acordo com o tipo de serviço (de 0 até 15). **log:** Quando a ACL é aplicada, uma mensagem informativa é impressa. **seq:** É o número de sequência e pode ser setado de modo manual ou automático. No modo manual, devem ser utilizados valores de 1 a 9999999, enquanto que no modo automático este número será incrementado de 10 a cada entrada da lista. Se uma lista é criada sem o seq-number após uma lista com o seq-numberespecificado, a nova lista assume como seq-number o próximo múltiplo de 10. **Exemplo:** Saída do comando **show access-lists** Extended IP access list 150 10 permit tcp any any **← seq não especificado** 12 permit eigrp any any **← seq=12**

	4) UDP CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE| resequence start-number increment-value | seq seq-number} udp {host host-ip | source source source-wildcard | any} [operator [port]]{host host-ip | destination destination-wildcard | any} [operator [port]] [precedence precedence] [tos tos] [log] [dscp dscp_mark] [fragments] [time-range WORD]	20 permit ospf any any **← seq não especificado** **resequence:** Reconfigura os valores de seq. **Exemplo:** CPE (config)# access-list 120 resequence 15 5 **← Inicia a ACL em 15 e incrementa cada nova entrada da lista em 5**. **remark:** Insere um comentário **<u>Operator:</u>** Compara portas de origem ou de destino. **lt:** A ACL será aplicada se o número da porta é menor que ou igual ao valor especificado após le
	5) SCTP CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE | resequence start-number increment-value | seq seq-number} sctp {host host-ip | source source source-wildcard | any} [operator [port]] {host host-ip | destination destination-wildcard | any} [operator [port]] [precedence precedence] [tos tos] [log] [dscp dscp_mark] [fragments] [time-range WORD] 6) IGMP CPE (config)# access-list access-list-number {permit | deny | remark remark_LINE | resequence start-number increment-value | seq seq-number} igmp {host host-ip | source source source-wildcard | any} {host host-ip | destination destination-wildcard | any} [precedence precedence] [tos tos] [log] [dscp dscp_mark] [fragments] [time-range WORD] **Exemplo 1:** CPE (config)# access-list 101 permit ip any 192.168.11.0 0.0.0.255 **Exemplo 2:** (config)# access-list 120 permit tcp host 192.168.100.20 eq 23 192.168.200.0 0.0.0.255	**gt:** A ACL será aplicada se o número da porta é maior que ou igual ao valor especificado após ge. **eq:** A ACL será aplicada se o número da porta é igual ao valor especificado após eq. **neq:** A ACL será aplicada se o número da porta é diferente ao valor especificado após neq. **range:** A ACL será aplicada se o número da porta esta entre o valores do range. No exemplo 1, todas as máquinas têm acesso livre a rede 192.168.11.0. Já no exemplo 2, a máquina com IP 192.168.100.20 tem o acesso via TELNET liberado para a rede 192.168.200.0/24. Ao final das duas listas tem-se implícita a linha **deny any**. Para remover uma ACL estendida usa-se: **no access-list access-list-number** **no access-list {access-list-number | sequence-numbers}**

4.7.2. Network Address Translation – NAT

O NAT (Network Address Translation) (RFC 1631) (RFC 1918) (RFC 2663) surgiu como uma alternativa para o problema da falta de endereços IPv4 na Internet. Para acessar a Internet, cada computador precisaria de um endereço IPv4 válido, fazendo com que os endereços existentes não fossem suficientes. Com o uso do NAT, os computadores da rede Interna utilizam os chamados endereços privados e para acessar a internet, tem os mesmos traduzidos para o endereço atribuído pelo ISP. As configurações de NAT são mostradas a seguir.

4.7.2.1. Permitindo o acesso de usuários internos à Internet

O PAT – Port Address Translation (ouNAT overload) permite que múltiplos usuários da LAN acessem a Internet, representados por um pequeno range de endereços IP, ou até mesmo um único endereço. Este recurso associa cada IP interno com uma porta TCP ou UDP junto ao IP válido e estas portas permitem que as conexões de IP's internos sejam identificadas e, deste modo, tenham um fluxo bidirecional. As configurações de NAT para estes casos são mostradas abaixo.

Tabela 43: Comandos para configuração de NAT da rede interna para a Internet.

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# ip nat pool pool-word first-addrlast-addr **Exemplo:** CPE (config)# ip nat pool POOL1 192.168.200.10 192.168.200.18	(Opcional) Cria um pool de endereços. Para remover um pool usa-se: **no ip nat pool pool-word**
4	CPE (config)# access-list acl-number permit ip netw-addr wildcard any **Exemplo:** CPE (config)# access-list 150 permit ip192.168.11.0 0.0.0.255 any	Cria uma ACL para definir quais os endereços internos que podem ser mapeados. Para remover a ACL: **no access-list acl-number**

5	CPE (config)# [no] ip nat inside source list acl-number {pool pool-word | interface type number} [overload] **Exemplos:** 1) Com pool de endereços CPE (config)# ip nat inside source list 150 pool POOL1 overload 2) Com um único endereço CPE (config)# ip nat inside source list 150 interface ethernet 1 overload	Configura uma access-list (que referencia uma rede interna) para ter seus endereços de host mapeados para um pool ou para o endereço de uma interface. Traduz o endereço fonte de pacotes IP que trafegam no no sentido inside → ouside (ex. Traduz um endereço da rede interna em um endereço atribuído pelo ISP). Traduz o endereço de destino daqueles que trafegam no sentido outside → inside (ex. traduz o endereço do ISP originalmente indicado como destino de um pacote proveniente da internet em um endereço da rede interna, associado a máquina que iniciou a comunicação). **Overload:**Garante que diversas máquinas da rede interna possam acessar a Internet através de um único endereço IP válido ou de um range de endereços válidos. Para remover a configuração usa-se o **no** a frente do comando.
6	CPE (config)# interface typenumber ip nat {inside | outside} **Exemplo:** CPE (config)# interface ethernet 0 CPE (config-ethernet0)# ip nat inside CPE (config-ethernet0)# exit CPE (config)# interface ethernet 1 CPE (config-ethernet1)# ip nat outside CPE (config-ethernet1)# exit	Acessa o modo de configuração da interface. No exemplo, configura a tradução de endereços no sentido inside → outside. **ip nat inside** deve ser configurado na interface por onde ingressam os pacotes que deverão ter seu endereço fonte traduzido. A interface por onde são enviados os pacotes com endereço de destino traduzido deve ter **ip nat outside** configurado. Para remover a configuração de NAT em uma interface: **no ip nat {inside | outside}**

4.7.2.2. Permitindo o acesso à dispositivos internos a partir da Internet

Em algumas situações é necessário permitir que dispositivos na Internet iniciem a comunicação com dispositivos da rede interna, como por exemplo, nos acessos a dispositivos via protocolos SSH e Telnet. Os procedimentos para configuração do NAT para estes casos são apresentadas a seguir.

Tabela 44: Configurações de NAT da Internet para a rede interna

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# ip nat outside destination static {tcp| udp} global-port local-addr local-port **Exemplo:** CPE (config)# ip nat outside destination static tcp 22000 192.168.11.2 22	Traduz o endereço de destino:porta de pacotes IP que trafegam no sentido outside → inside (ex. traduz o endereço do ISP originalmente indicado como destino de um pacote proveniente da internet em endereço: porta da rede interna). Traduz o endereço fonte de pacotes IP que trafegam no sentido inside → ouside (ex. Traduz um endereço da rede interna em um endereço atribuído pelo ISP). No exemplo, um acesso feito a partir da Internet para um o IP da interface conectada ao ISP para a porta 22000 terá o endereço de destino substituído por 192.168.11.2:22.
4	CPE (config)# interface typenumber **Exemplo:** CPE (config)# interface ethernet 1 CPE (config-ethernet1)# ip nat outside CPE (config-ethernet1)# exit CPE (config)# interface ethernet 0 CPE (config-ethernet0)# ip nat inside CPE (config-ethernet0)# exit	Acessa o modo de configuração da interface. No exemplo, configura a tradução de endereços no sentido outside → inside. **ip nat outside** deve ser configurado na interface por onde ingressam os pacotes que deverão ter seu endereço de destino traduzido. A interface por onde são enviados os pacotes com endereço de destino traduzido deve ter **ip nat inside** configurado.

4.7.3. Unicast Reverse Path Forwarding- URPF

O Unicast Reverse Path Fowarding é um mecanismo de segurança utilizado em roteadores para verificar se o endereço fonte dos pacotes que ingressam através de suas interfaces é alcançável. Este mecanismo contribui para limitar a ocorrência de endereços falsos (spoofing) na rede. Se o endereço fonte não é válido, o pacote é descartado.

O URPF pode atuar nos modos strict ou loose. No modo strict um pacote deve ser recebido na mesma interface que o roteador utiliza para enviar o respectivo retorno. Pode ocorrer o descarte de pacotes legítimos se estes ingressarem em uma interface diferente da que é normalmente escolhida pelo roteador para enviar o tráfego de retorno. Já no modo loose o endereço fonte deve constar na tabela de roteamento para não ser descartado.

A tabela abaixo apresenta os comandos para configuração de URPF:

Tabela 45: Configuração de URPF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração global.
3	CPE (config)# interface *type number*	Acessa o modo de configuração da interface.
4	CPE (config-*interface*)# ip | ipv6 verify unicast source {rx | any}	(Opcional) O URPF deve ser habilitado diretamente na interface onde se deseja que seja feita a verificação. O comando <**ip | ipv6> verify unicast source rx** habilita o URPF em modo rigoroso (*strict*), enquanto que o comando <**ip | ipv6> verify unicast source any** habilita o modo menos severo (*loose*) do URPF.

4.8. Roteamento

Esta seção apresenta os comandos para configuração de rotas estáticas e dos protocolos de roteamento RIP (RFC 1058) (RFC 2453) (RFC 4822), OSPF (RFC 2328), BGP (RFC 4271) e PIM (RFC 2362).

4.8.1. Adição de Rotas Estáticas

Os procedimentos para adição de rotas estáticas são descritos abaixo:

Tabela 46: Configuração de rotas estáticas

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# [no] ip route [vrf vrf-name] netw-addr/mask{gateway-addr |bridge number| dialer number | ethernet number |loopbacknumber | nexthop-vrf vrf_name | null | tunnel number} [distance distance_value] CPE(config)# [no] ip route static{ bfd {ethernet *number gateway-addr*| tunnel *number gateway-addr*}| inter-vrf} CPE(config)# [no] ip route vrf *vrf_name netw-addr/mask* {*gateway-addr* | bridge *number* | dialer *number* | *e*thernet *eth_number* | loopback lo_number | nexthop-vrf *vrf_name* | null | tunnel *number*} [distance distance_value] **Exemplo:** CPE (config)# ip route 192.168.90.0/24 192.12.5.7CPE(config)# [no] ip route netw-addr/mask{gateway-addr |bridge number| dialer number | ethernet number |loopbacknumber | nexthop-vrf vrf_name | null | tunnel number} [distance distance_value] CPE(config)# [no] ip route static{ bfd {ethernet number gateway-addr| tunnel number gateway-addr}| inter-vrf} CPE(config)# [no] ip route vrf vrf_name netw-addr/mask {gateway-addr | bridge number | dialer number | ethernet eth_number | loopback lo_number | nexthop-vrf vrf_name | null | tunnel number} [distance distance_value] **Exemplo:** CPE (config)# ip route 192.168.90.0/24 192.12.5.7	Adiciona ou remove uma rota estática, configurando como próximo salto um endereço ou uma interface (dialer, ethernet ou loopback).

4.8.2. Routing Information Protocol – RIP

O RIP (Routing Information Protocol) (RFC 1058) (RFC 2453) (RFC 4822) é um protocolo baseado em vetor distância, que utiliza como métrica para roteamento a contagem de saltos, para medir a distância entre a rede de origem e a de destino. O roteador informa aos seus vizinhos a sua tabela de roteamento através de mensagens de atualização enviadas sobre UDP broadcast (na versão 1) ou multicast (na versão 2), em intervalos regulares de tempo ou quando ocorrem alterações na topologia da rede. O número máximo de hops em um caminho é 15. Se um roteador recebe em uma atualização uma entrada nova ou alterada cuja métrica seja maior do que 15, a rede de destino é considerada inalcançável.

Em relação à segurança, a segunda versão do RIP implementa autenticação através de texto aberto e MD5.

Abaixo são mostradas as configurações do RIP:

Importante: A inscrição“Opcional” indica que o comando não é obrigatório para o funcionamento básico do protocolo.

Tabela 47: Configuração do protocolo RIP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router rip [vrf vrf-name]	Acessa o modo de configuração do protocolo RIP. Opcionalmente, configura o RIP para uma VRF específica. Para desabilitar o roteador RIP usa-se: **no router rip**
4	CPE (config-rip)# [no] network {netw-addr/mask | bridge number | dialer number | ethernet number | tunnel number}	Define quais as redes serão associadas ao processo de roteamento RIP. Para remover uma rede previamente configurada usa-se o **no** a frente do comando.
5	CPE (config-rip)# [no] neighbor ip-addr	(Opcional) O RIP, em seu modo normal de operação, envia as atualizações em broadcast. O comando **neighbor** define um roteador vizinho para a troca de informações de roteamento, podendo ser usado para permitir que tais informações alcancem redes que não suportam broadcasts. Para remover um neighbor usa-se o **no** a frente do comando.
6	CPE (config-rip)# [no] redistribute {bgp | connected | kernel | ospf | static} [metric metric]	(Opcional) Configura a redistribuição de rotas, podendo definir uma métrica com valor de 1 até 16 para o tipo de rota que será redistribuída. Para remover a redistribuição, usa-se o **no** a frente do comando.

7	CPE (config-rip)# [no] default-information originate	(Opcional) Gera uma rota default no protocolo RIP. Para remover esta rota, deve ser utilizado [no].
8	CPE (config-rip)# [no] default-metric metric	(Opcional) Especifica ou remove uma métrica para as rotas que serão redistribuídas, com valor de 1 até 16.
9	CPE (config-rip)# [no] passive-interface { bridge number|default | dialer number | ethernet number | tunnel number}	(Opcional) Suprime as atualizações de rotas em uma interface. Para remover a configuração, usa-se o **no** a frente do comando.
10	CPE (config-rip)# timers basic update timeout garbage-collection	(Opcional) Ajusta os timers do protocolo (para envio de atualizações, timeout e limpeza das informações, respectivamente). Os valores default para estes timers são respectivamente 30, 180 e 120 segundos. Para remover a configuração de timers: **no timers basic**
11	CPE (config-rip)# [no] version {1 | 2}	(Opcional) Configura / remove a configuração da versão do RIP para envio e recebimento de pacotes. Por default, ao habilitar o roteador RIP o mesmo é configurado para enviar a versão 2 e receber as versões 1 e 2 do protocolo.
12	CPE (config-interface)# [no] ip rip {send | receive} version {1 | 2}	(Opcional) Configura em uma interface o envio ou recebimento de pacotes de uma versão do RIP para envio e recebimento de pacotes. Para remover a configuração: **no ip rip {send | receive} version**
13	CPE(config-*interface*)# [no] ip rip authentication {key-chain *key-chain-name* | mode {md5 [auth-length rfc]| text} | string *string*} **Exemplo:** CPE(config-ethernet1)# ip rip authentication key-chain RIP CPE(config-ethernet1)# ip rip authentication mode md5 CPE(config-ethernet1)# exit CPE(config)# key chain RIP CPE(config-keychain) # key 1 CPE(config-keychain-key)# key-string secret	(Opcional) Habilita/desabilita o uso de autenticação no RIP. Válido somente para a versão 2. O exemplo mostra os passos para configuração da autenticação do RIP na interface ethernet 0, com uso do padrão MD5.
14	CPE (config-interface)# [no] ip split-horizon [poisoned-reverse]	(Opcional) Habilita/desabilita o split horizon. O split-horizon evita loops no roteamento por que evita que uma rota seja propagada pelo caminho através do qual ela foi aprendida.

4.8.3. Open Shortest Path First – OSPF

O OSPF (RFC 2328) é um protocolo baseado no algoritmo SPF (Shortest Path First), também conhecido como algoritmo de Dijkstra. Este protocolo pode operar com hierarquias, sendo que a maior entidade dentro da hierarquia é o sistema autônomo (Autonomous System, AS), que é um conjunto de redes sob mesma administração.

O OSPF é um protocolo de roteamento intra-AS, do tipo link-state, que envia avisos referentes ao estado da conexão (os LSAs – Link State Advertisements) a todos os outros roteadores pertencentes a mesma área hierárquica, permitindo que os roteadores mantenham bases de dados com informações sobre o estado dos enlaces e utilizem o algoritmo SPF para calcular o caminho mais curto para cada destino. O tipo de LSA empregado varia de acordo com seu propósito (anúncio para uma mesma área ou para outra área, por exemplo).

Em uma rede OSPF são encontrados os seguintes tipos de roteadores:

- **Internal**- Possui todas as suas interfaces em uma mesma área.
- **Backbone** - Um roteador do tipo internal contido na área 0 (Backbone Area).
- **Area Border Router (ABR)** - Possui pelo menos uma interface na Area 0 e as demais em quaisquer outras áreas. Os ABRs podem realizar a sumarização de rotas.
- **Autonomous System Border Router (ASBR)** - Realiza a redistribuição de rotas de outras fontes para dentro do domínio OSPF. Pode realizar sumarização de rotas.

Dentro de uma área, para evitar tráfego excessivo na sincronização das bases de dados entre os roteadores OSPF, é utilizado um roteador chamado Designated Router (DR), escolhido automaticamente,cujo papel é trocar informações com todos os outros roteadores pertencentes a sua área. Também é escolhido um BackupDesignated Router (BDR), que assume em caso de falha do DR.

A tabela mostra as configurações do protocolo OSPF.

Importante:

A inscrição “Opcional” indica que o comando não é obrigatório para o funcionamento básico do protocolo.

Tabela 48: Configurações do protocolo OSPF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] router ospf [vrf vrf-name]	Acessa o modo de configuração do protocolo OSPF. Opcionalmente, configura o OSPF para uma VRF específica. Para remover a configuração, usa-se o **no** a frente do comando.
4	CPE (config-ospf)# [no] network netw-addr/mask area area-id **Exemplo:** CPE (config-ospf)# network 192.168.100.0/24area 0.0.0.0 CPE (config-ospf)# network 192.168.220.0/24area 2.2.0.0	Configura o roteador para enviar/receber pacotes OSPF nas interfaces conectadas as redes especificadas com o comando **network.** Cada rede deve ser associada a uma área, sendo que nos casos mais simples podem-se ter todas as redes pertencendo a mesma área (área 0 ou backbone). Para a área são aceitos valores de 0 até 4294967295 ou no formato de endereço Ipv4. Para remover uma área usa-se **no** na frente do comando.
5	CPE (config-ospf)# [no] neighbor ip-addr [pool-interval pool-int][priority priority]	(Opcional) O OSPF, em seu modo normal de operação, envia as atualizações em broadcast. O comando **neighbor** define um roteador vizinho para a troca de informações de roteamento, podendo ser usado para permitir que tais informações alcancem redes que não suportam broadcasts. Para remover um neighbor usa-se **no** na frente do comando. **Importante:** Em links ponto-multiponto, em redes com suporte a broadcasts não existe necessidade de especificar vizinhos, visto que todas as mensagens são enviadas em multicast. Nas redes ponto-multiponto sem suporte a broadcast é indispensável que os vizinhos OSPF sejam especificados.
6	CPE (config-ospf)# [no] redistribute {bgp | connected | kernel | rip| static} [metric metric] [metric-type type]	(Opcional) Configura a redistribuição de rotas (ou remove a configuração) aprendidas de outras fontes no OSPF. **Parâmetros:** **metric:** Métrica default para redistribuição de rotas OSPF, com valores de 0 até 16777214. **metric-type:** métrica OSPF do tipo external 1 ou 2.

7	CPE (config-ospf)# default-information originate[always] [metric metric] [metric-type type]	(Opcional) Gera uma rota default no protocolo OSPF. Para remover esta rota, deve ser utilizado [no].
8	CPE (config-ospf)# default-metric metric.	(Opcional) Especifica uma métrica para as rotas que serão redistribuídas (de 0 até 16777214).
9	CPE (config-ospf)# timers throttle spf delay init-hold-time max-hold-time	(Opcional) Ajusta os timers do algoritmo SPF, possibilitando seu escalonamento em intervalos da ordem de milissegundos e pode ser utilizado para retardar os cálculos do SPF nos momentos de instabilidade da rede. Este algoritmo é usado para calcular a SPT (Shortest Path Tree)quando ocorrem mudanças na topologia da rede. **Parâmetros:** **delay:** Tempo contado a partir da primeira mudança recebida até o momento do cálculo do SPF. **Init-hold-time:** Tempo inicial de espera entre os cálculos consecutivos do SPF. **max-hold-time:** Tempo inicial de espera entre os cálculos consecutivos do SPF Os valores para estes timers devem ser de 0 até 600000 **mili**segundos.
10	CPE (config-ospf)# auto-cost reference-bandwidth bandwidth	(Opcional) Configura a largura de banda de referência em Mbits por segundo. Para remover a configuração: **no auto-cost reference-bandwidth**
11	CPE (config-ospf)# [no] capability opaque	(Opcional) Habilita/desabilita o envio de Opaque LSAs (RFC 5250). Este tipo de LSA provê um mecanismo generalizado para suportar futuras extensões do OSPF, sendo atualmente utilizado em OSPF-TE (Traffic Engineering) (RFC 3630) (RFC 4203) (RFC 5786).
12	CPE (config-ospf)# distance administrative-distance | ospf {external value | inter-area value | intra-area value}	(Opcional)Uma distância administrativa é uma classificação da confiabilidade de uma fonte de informações de roteamento. A distância administrativa é um inteiro entre 0 e 255 e quanto maior o valor, menor é a confiança. Uma fonte com distância de 255 não é confiável e por este motivo deve ser ignorada. O OSPF usa três diferentes distâncias administrativas: intra-área, inter-área e externa. Rotas dentro de uma área são intra-área; rotas para outra área estão inter-área, e rotas de outro domínio de roteamento que são redistribuídas são externas. A distância default para cada um destes tipos é 110. Os valores configurados devem ser de 1 até 255. Para remover a configuração: **no distance {administrative-distance | ospf}**

4.8.3.1. Configurações específicas de área no OSPF

A tabela mostra os procedimentos para configuração de parâmetros opcionais para as áreas OSPF.

Tabela 49: Configuração dos parâmetros de área OSPF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router ospf	Acessa o modo de configuração do protocolo OSPF.
	CPE(config-ospf)# area *area-id* authentication [message-digest *KEY*]	(Opcional) Configura a autenticação MD5 em uma área OSPF. É necessário configurar a chave na interface associada a área onde se deseja a autenticação. *** Importante: Configurações de autenticação feitas nas interfaces sobrescrevem as configurações de atenticação nas áreas**
	CPE (config-ospf)# area area-id export-list lista	(Opcional) Define um filtro para as redes que serão anunciadas para outras áreas, tendo efeito exclusivamente sobre os summary LSAs tipo 3 (anúncios de rotas internas da área especificada).
	CPE (config-ospf)# area area-id filter-list prefix prefix-list {in | out}	(Opcional) Define um filtro para summary LSAs tipo 3 enviados entre áreas através do uso de prefix-lists. Esta opção deve ser usada em Area Border Routers (ABRs) somente.
	CPE (config-ospf)# area area-id import-list list	(Opcional) Define um filtro para as redes que são anunciadas a partir de outras áreas para a área especificada, tendo efeito exclusivamente sobre os summary LSAs tipo 3.
	CPE (config-ospf)# area area-id stub [no-summary]	(Opcional) Configura uma área como stub.
	CPE (config-ospf)# area area-id nssa [translate-always | translate-candidate | translate-never] [no-summary]	(Opcional) Configura uma área como Not-so-Stub Area (NSSA) (RFC 3101).
	CPE (config-ospf)# area area-id default-cost cost	(Opcional) Configura o custo dos default-summary LSAs anunciados para as áreas stub (de 0 até 16777215).
	CPE (config-ospf)# area area-id range netw-addr/mask [advertise [cost cost] | cost cost | not-advertise | substitute netw-addr/mask] **Exemplo:** CPE (config-ospf)# area 10 range 10.0.0.0/8 substitute 11.0.0.0/8	(Opcional) Sumariza as rotas com endereço e máscara especificados (somente LSAs dos tipos 1 e 2 rotas intra-área) em um LSA tipo 3. Este comando deve ser utilizado somente em Area Border Routers (ABRs). No exemplo, um LSA tipo 3 com a rota 11.0.0.0/8 é enviado para a área backbone se a area 10 contém pelo menos uma rede intra-area (descrita com LSAs tipo 1 ou 2) do range 10.0.0.0/8.
	CPE (config-ospf)# area area-id shortcut {default | disable | enable}	(Opcional) Habilita o modo shortcut para a área especificada.

4.8.3.2. Criação de virtual links

No protocolo OSPF, todas as áreas devem ser conectadas a área 0 (backbone). Se houver uma quebra de continuidade backbone, é possível estabelecer uma conexão virtual (virtual link) (RFC 5185). Os dois pontos finais de um link virtual devem ser Area Border Routers e o virtual link deve ser configurado em ambos os roteadores, considerando-se a área comum entre eles.

A tabela mostra os passos para criação de virtual links.

Tabela 50: Criação de virtual links

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router ospf	Acessa o modo de configuração do protocolo OSPF.
4	CPE (config-ospf)# area area-id virtual-link router-id **Exemplo:** CPE (config-ospf)# area 1virtual-link192.168.12.1	Cria um virtual link. No exemplo cria-se um virtual link entre o roteador local e o roteador com IP 192.168.12.2, sendo que ambos têm uma interface na área 1. Se a área 1 do exemplo for conectada a área 0 e se existir uma área 2 conectada a área 1, será possível interligar as áreas 2 e 0 através do uso deste virtual link.
5	CPE (config-ospf)# area area-id virtual-link router-id [dead-interval seconds | hello-interval seconds | retransmit-interval seconds | transmit-delay seconds]	(Opcional) Ajusta os timers para o virtual link. **Parâmetros:** **dead-interval:** Intervalo após o qual um vizinho passa a ser considerado inativo. **hello-interval:** Intervalo entre os pacotes hello na interface OSPF associada ao virtual link. **retransmit-interval:** Especifica o intervalo entre as retransmissões dos LSAs (notificações de estado de link) na interface OSPF associada ao virtual link. **transmit-delay:** Especifica o intervalo para envio de pacotes link state update na interface OSPF associada ao virtual link.
6	CPE (config-ospf)# area area-id virtual-link router-id authentication	(Opcional) Cria um virtual link. Deve-se definir também a senha para autenticação, conforme o passo 7. *** Importante: Configurações de autenticação feitas nas interfaces sobrescrevem as configurações de autenticação nas áreas.**
7	CPE (config-ospf)# area area-id virtual-link router-id authentication-key key	(Opcional) Cria um virtual link e define uma senha em texto aberto para ser utilizada pelos roteadores que estão nas pontas do virtual link.

8	CPE (config-ospf)# area area-id virtual-link router-id authentication authentication-key key	(Opcional) Cria um virtual link e define o uso de autenticação através de uma senha em texto aberto (parâmetro **key**) nos roteadores que estão nas pontas do virtual link.
9	CPE (config-ospf)# area area-id virtual-link router-id authentication message-digest	(Opcional) Cria um virtual link e define o uso de autenticação através de MD5 nos roteadores que estão nas pontas do virtual link. É necessário definir também a senha para autenticação, conforme o passo 10.
10	CPE (config-ospf)# area area-id virtual-link router-id message-digest-key key-id md5 key	(Opcional) Cria um virtual link e define o uso de uma senha para autenticação via MD5 nos roteadores que estão nas pontas do virtual link. O key-id deve assumir valores de 1 até 255 e é enviado no pacote OSPF juntamente com o hash MD5 e com um número de sequência que não pode ser decrescente.
11	CPE (config-ospf)# area area-id virtual-link router-id authentication message-digest authentication-key key	(Opcional) Cria um virtual link e habilita a autenticação via MD5 entre os roteadores que estão nas pontas do virtual link, definindo a senha para autenticação.
12	CPE (config-ospf)# area area-id virtual-link router-id authentication message-digest message-digest-key key-id md5 key	(Opcional) Cria um virtual link e habilita a autenticação via MD5 entre os roteadores que estão nas pontas do virtual link, definindo uma senha para autenticação via MD5 nos roteadores que estão nas pontas do virtual link. O key-id deve assumir valores de 1 até 255 e é enviado no pacote OSPF juntamente com o hash MD5 e com um número de sequência que não pode ser decrescente.

4.8.3.3. Configuração de parâmetros do OSPF nas interfaces

A tabela a seguir mostra os procedimentos para configuração de parâmetros nas interfaces que tem OSPF habilitado.

Tabela 51: Configuração de parâmetros OSPF na interface

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number	Acessa o modo de configuração da interface.

4	CPE (config-interface)# [no] ip ospf authentication [interface-ipaddr | message-digest[interface-ipaddr] | null[interface-ipaddr]]	(Opcional) Configura a autenticação MD5 na interface ou desabilita o uso de autenticação.
	CPE (config-interface)#[no] ip ospf authentication-key key	(Opcional) Configura uma senha para ser utilizada pelos roteadores OSPF vizinhos em um segmento de rede que utiliza autenticação por senha no OSPF.
	CPE (config-interface)# [no] ip ospf cost cost	(Opcional) Define o custo (ou métrica) da interface. O custo de uma interface no OSPF indica o overhead necessário para enviar pacotes através da mesma. Este custo é inversamente proporcional a largura de banda da interface. Uma largura de banda maior implica em um custo menor. A fórmula utilizada para calcular o custo é: **custo = 10000 0000/largura de banda (bps)**
	CPE (config-interface)# [no] ip ospf {dead-interval {seconds | minimal hello-multiplier number | hello-interval seconds | retransmit-interval seconds | transmit-delay seconds}	(Opcional) Ajusta os timers do OSPF na interface. **Parâmetros:** **dead-interval:** Intervalo após o qual um vizinho passa a ser considerado inativo. **hello-interval:** Intervalo entre os pacotes hello. **retransmit-interval:** Especifica o intervalo entre as retransmissões dos LSAs (notificações de estado de link). **transmit-delay:** Especifica o intervalo para envio de pacotes link state update.
	CPE (config-interface)# [no] ip ospf message-digest-key key-id md5 key	(Opcional) Define uma senha para autenticação via MD5. O key-id deve assumir valores de 1 até 255 é enviado no pacote OSPF juntamente com o hash MD5 e com um número de sequência que não pode ser decrescente.
	CPE (config-interface)# [no] ip ospf mtu-ignore	(Opcional) Desabilita a detecção de incompatibilidade no MTU (MaximumTransferUnit).
	CPE (config-interface)# ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	Define o tipo de rede para uma interface. **Opções:** **broadcast:** Especifica uma rede OSPF multiacesso com suporte a broadcasts para a interface. **non-broadcast:** Especifica uma rede OSPF sem suporte a broadcasts para a interface. **point-to-multipoint:** Especifica uma rede OSPF ponto-multiponto para a interface. **Point-to-point:** Especifica uma rede OSPF ponto-a-ponto para a interface.

	CPE (config-interface)# ip ospf priority priority	(Opcional) Define a prioridade do roteador, cujo valor deve ser de 1 até 255. Esta prioridade é utilizada para a eleição do Designated Router (DR) e do Backup Designated Router (BDR), que é feita através do envio (em multicast) de pacotes Hello. O roteador com mais alta prioridade se torna o DR. O mesmo acontece com o BDR. Na ocorrência de empate, o roteador com maior router id vence. O router id é o maior IP entre todas as interfaces do roteador, incluindo a loopback.

4.8.3.4. Verificação das informações do OSPF

A tabela abaixo mostra os comandos para verificação das informações de roteamento do OSPF.

Tabela 52: Verificação das informações de roteamento do OSPF

Comando	Objetivo
CPE# show ip ospf border-routers	Mostra as informações relacionadas ao ABR (Area Border Router) e ao ASBR (Autonomous System Boundary Router).
CPE# show ip ospf database [asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary | self-originate] [adv-router link-state-id | self-originate] | [asbr-summary link-state-id [adv-router link-state-id | self-originate]]	Mostra os LSAs (Link State Advertisements), podendo os mesmos serem filtrados com base na origem (roteador local ou link state ID do roteador).
CPE# show ip ospf database max-age	Exibe os LSAs que estão na listagem max age.
CPE# show ip ospf interface {bridge number | dialer number | ethernet number| tunnel number }	Mostra as informações sobre as interfaces com OSPF.
CPE# show ip ospf neighbor [neighbor-id | all |bridge number | detail | dialer number | ethernet number | tunnel number]	Mostra as informações relacionadas aos neighbors OSPF.
CPE# show ip ospf route	Exibe a tabela de rotas OSPF.

4.8.3.5. Configuração de BFD no OSPF

A tabela abaixo mostra os comandos para configuração do BFD (Bidirectional Forwarding Detection) no OSPF.

Tabela 53: Comandos para configuração do BFD no OSPF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)#interface type number	Acessa o modo de configuração da interface.
4	CPE(config-*interfacenum*)# ip ospf bfd	(Opcional) Habilita a detecção de falhas através do BFD na interface. Este comando deve ser executado nas interfaces que estão associadas ao processo OSPF. **Importante:** É fundamental configurar os timers do BFD conforme consta na seção **"Bidirectional Forwarding Detection – BFD"**.

Comandos Relacionados

CPE# show bfd neighbors	Exibe informações sobre os neighbors BFD, tais como endereço IP, quantidade de pacotes recebidos e enviados, e estado (up/down).

4.8.3.6. OPAQUE LSA

OSPF Opaque LSAs asão utilizado juntamente com MPLS-TE. Embora o CPE não possua MPLS TE, há o suporte das extensões de engenharia de tráfego para OSPF (RFC2630) para que o roteador acima (PE) possa se valer das informações. Os OPAQUE LSA (Link-State Advertisement) são definidos pelas RFC5250 (que obsoletou a RFC 2370) e compreendem os tipos 9, 10 e 11 de LSA, que são respectivamente ao escope de link-local, area-local e AS. São usados para transportar dados da utilização do link de cada interface.

Tabela 54: Comandos para configuração dos OPAQUE LSA no OSPF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# router ospf	Acessa o modo de configuração do protocolo OSPF.
4	CPE(config-ospf)# capability opaque	Habilita o envio de Opaque LSAs.
5	CPE(config-ospf)# mpls traffic-eng	Habilita as extensões de engenharia de tráfego do OSPF, através dos Opaque LSA.
6	CPE(config-ospf)# mpls traffic-eng router-address A.B.C.D	(Opcional) Estabelece um ip estável do roteador que estiver fazendo os anúncios.
7	CPE(config-ospf)# exit	Sai da configuração do ospf
8	CPE(config)#interface *type number*	Acessa o modo de configuração da interface.
9	CPE(config-*interfacenum*)# mpls traffic-eng administrative-weight *weight*	(Opcional) Sobreescreve o peso IGP do link
10	CPE(config-*interfacenum*)# mpls traffic-eng attribute-flags *flags*	(Opcional) Especificações do usuário para comparar com o atributo *affinity* no estabelecimento dos túneis
11	CPE(config-*interfacenum*)# mpls traffic-eng link [max-bw *bw* | max-rsv-bw *bw* | unrsv-bw *prio bw*]	(Opcional) Define limites de bandas máxima (max-bw), máxima reservada(max-rsv-bw) e não-reservada (unrsv-bw) para o link. Os detalhes dos sub-TLV podem ser encontrados na seção 2.5 da RFC3630.

4.8.4. Open Shortest Path First v3– OSPFv3

O OSPFv3 (RFC5340) é uma extensão do protocolo OSPFv2 baseado no algoritmo SPF *(Shortest Path First)*, também conhecido como algoritmo de Dijkstra, tento suporte para IPV6. Este protocolo pode operar com hierarquias, sendo que a maior entidade dentro da hierarquia é o sistema autônomo (*Autonomous System, AS)*, que é um conjunto de redes sob mesma administração.

O OSPF é um protocolo de roteamento intra-AS, do tipo *link-state*, que envia avisos referentes ao estado da conexão (os LSAs – *Link State Advertisements*) a todos os outros roteadores pertencentes a mesma área hierárquica, permitindo que os roteadores mantenham bases de dados com informações sobre o estado dos enlaces e utilizem o algoritmo SPF para calcular o caminho mais curto para cada destino. O tipo de LSA empregado varia de acordo com seu propósito (anúncio para uma mesma área ou para outra área, por exemplo).

Em uma rede OSPF são encontrados os seguintes tipos de roteadores:

- ***Internal***- Possui todas as suas interfaces em uma mesma área.
- ***Backbone*** - Um roteador do tipo *internal* contido na área 0 *(Backbone Area)*.
- ***Area Border Router (ABR)*** - Possui pelo menos uma interface na Area 0 e as demais em quaisquer outras áreas. Os ABRs podem realizar a sumarização de rotas.
- ***Autonomous System Border Router (ASBR)*** - Realiza a redistribuição de rotas de outras fontes para dentro do domínio OSPF. Pode realizar sumarização de rotas.

Dentro de uma área, para evitar tráfego excessivo na sincronização das bases de dados entre os roteadores OSPF, é utilizado um roteador chamado *Designated Router (DR)*, escolhido automaticamente, cujo papel é trocar informações com todos os outros roteadores pertencentes a sua área. Também é escolhido um *Backup Designated Router (BDR)*, que assume em caso de falha do DR.

O OSPFv3 intruduz dois novos tipos de LSA: *LINK* e *Intra-area prefix*. Uma das maiores vantagens do OSPFv3 sobre a versão 2 é a separação do endereçamento IP para o cálculo da árvore SPF. Isso faz com que alterações de endereçamento não afetem a integridade da árvore e evitam o recálculo da mesma.

O OSPFv3 é compatível com a RFC 5643 para MIB. O OID para o ospf v2 é 1.3.6.1.3.102 de acordo com a OSPFV3-MIB.

A tabela mostra as configurações do protocolo OSPFv3.

Importante:
A inscrição "Opcional" indica que o comando não é obrigatório para o funcionamento básico do protocolo.

Tabela 55: Configurações do protocolo OSPFv3

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# [no] ipv6 router ospf [vrf vrf-name]	Acessa o modo de configuração do protocolo OSPFv3. Opcionalmente, configura o OSPFv3 para uma VRF específica. Para remover a configuração, usa-se o **no** a frente do comando.
4	CPE(config-ospf)# [no] interface iface area 0.0.0.0 **Exemplo:** CPE(config-ospf6)#interface loop 0 area 0.0.0.0 CPE(config-ospf6)# interface ethernet 1 area 2.2.0.0	Configura o roteador para enviar/receber pacotes OSPFv3 na interface selecionada. Cada rede deve ser associada a uma área, sendo que nos casos mais simples podem-se ter todas as redes pertencendo a mesma área (área 0(0.0.0.0) ou backbone). Para a área são aceitos valores no formato de endereço Ipv4. Para remover uma área usa-se **no** na frente do comando.
5	CPE(config-ospf6)# [no] router-id *IPV4*	(Opcional) Especifica o router-id do OSPFv3. Usualmente é utilizado o maior IP do sistema. Para remover um neighbor usa-se **no** na frente do comando.
6	CPE (config-ospf6)# [no] redistribute {bgp | connected | kernel | ripng | static} [metric *metric*] [metric-type *type*]	(Opcional) Configura a redistribuição de rotas (ou remove a configuração) aprendidas de outras fontes no OSPFv3. **Parâmetros:** **metric:** Métrica default para redistribuição de rotas OSPF, com valores de 0 até 16777214. **metric-type:** métrica OSPF do tipo *external* 1 ou 2.

4.8.4.1. Configurações específicas de área no OSPFv3

A tabela mostra os procedimentos para configuração de parâmetros opcionais para as áreas OSPFv3.

Tabela 56: Configuração dos parâmetros de área OSPFv3

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ipv6 router ospf	Acessa o modo de configuração do protocolo OSPFv3.
	CPE(config-ospf6)# area *area-id* export-list *lista*	(Opcional) Define um filtro para as redes que serão anunciadas para outras áreas, tendo efeito exclusivamente sobre os summary LSAs tipo 3 (anúncios de rotas internas da área especificada).
	CPE(config-ospf6)# area *area-id* filter-list prefix *prefix-list* {in | out}	(Opcional) Define um filtro para summary LSAs tipo 3 enviados entre áreas através do uso de prefix-lists. Esta opção deve ser usada em Area Border Routers (ABRs) somente.
	CPE(config-ospf6)# area *area-id* import-list *list*	(Opcional) Define um filtro para as redes que são anunciadas a partir de outras áreas para a área especificada, tendo efeito exclusivamente sobre os summary LSAs tipo 3.
	CPE(config-ospf6)# area *area-id* range *netw-addr/mask* [advertise [cost *cost*] | cost *cost* / not-advertise | substitute *netw-addr/mask*] **Exemplo:** CPE(config-ospf6)# area 0.0.0.10 range 10.0.0.0/8 substitute 11.0.0.0/8	(Opcional) Sumariza as rotas com endereço e máscara especificados (somente LSAs dos tipos 1 e 2 rotas intra-área) em um LSA tipo 3. Este comando deve ser utilizado somente em Area Border Routers (ABRs). No exemplo, um LSA tipo 3 com a rota 11.0.0.0/8 é enviado para a área backbone se a area 10 contém pelo menos uma rede intra-area (descrita com LSAs tipo 1 ou 2) do range 10.0.0.0/8.

4.8.4.2. Configuração de parâmetros do OSPFv3 nas interfaces

A tabela a seguir mostra os procedimentos para configuração de parâmetros nas interfaces que tem OSPFv3 habilitado.

Tabela 57: Configuração de parâmetros OSPF na interface

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface type number	Acessa o modo de configuração da interface.
	CPE(config-interface)# [no] ipv6 ospf cost cost	(Opcional) Define o custo (ou métrica) da interface. O custo de uma interface no OSPF indica o overhead necessário para enviar pacotes através da mesma. Este custo é inversamente proporcional a largura de banda da interface. Uma largura de banda maior implica em um custo menor. A fórmula utilizada para calcular o custo é: **custo = 10000 0000/largura de banda (bps)**
	CPE(config-*interface*)# [no] ipv6 ospf {dead-interval {*seconds* | minimal hello-multiplier *number* | hello-interval *seconds* | retransmit-interval *seconds* | transmit-delay *seconds*}	(Opcional) Ajusta os timers do OSPF na interface. **Parâmetros:** **dead-interval:** Intervalo após o qual um vizinho passa a ser considerado inativo. **hello-interval:** Intervalo entre os pacotes *hello.* **retransmit-interval:** Especifica o intervalo entre as retransmissões dos LSAs (notificações de estado de link). **transmit-delay:** Especifica o intervalo para envio de pacotes link state update.
	CPE (config-*interface*)# [no] ipv6 ospf mtu-ignore	(Opcional) Desabilita a detecção de incompatibilidade no MTU *(MaximumTransferUnit)*.
	CPE (config-*interface*)# [no] ipv6 ospf priority *priority*	(Opcional) Define a prioridade do roteador, cujo valor deve ser de 1 até 255. Esta prioridade é utilizada para a eleição do Designated Router (DR) e do Backup Designated Router (BDR), que é feita através do envio (em multicast) de pacotes Hello. O roteador com mais alta prioridade se torna o DR. O mesmo acontece com o BDR. Na ocorrência de empate, o roteador com maior router id vence. O router id é o maior IP entre todas as interfaces do roteador, incluindo a loopback.

4.8.4.3. Autenticação em links OSPFv3

Exite duas maneiras distintas de autenciação entre vizinhos OSPFv3. A primeira, mais antiga é parte a RFC4552, onde a autenciação é feita através de IPSec. Em alguns equipamentos onde não há ipsec ou o ipsec está habilitado por licença, há uma nova forma de autenticação estabelecida pela RFC6506.

A autenticação pela RFC4552 pode ser feita por área, ou por interface:

Tabela 58: Comandos para configuração da autenticação por interface, RFC 4552 no OSPFv3

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *iface num*	Acessa a interface que se deseja fazer a autenticação.
4	CPE(config-*ifacenum*)# ipv6 ospf encryption [ipsec spi *num* esp [3des *key* | aes-cbc *bits key* | des *key* | null] [md5 | sha1] *hashkey* ou CPE(config-*ifacenum*)# ipv6 ospf encryption null ou CPE(config-*ifacenum*)# ipv6 ospf authentication ipsec spi *num* [md5 | sha1] *hashkey*	Habilita o modo ipsec ESP de autenticação. Deve-se configurar o spi, a chave, o tipo de criptografia, o numero de bits da criptografia, o tipo de hash e a palavra do hash ou Habilita o modo null de encryption ou Habilita o modo ipsec AH de autenticação. Deve-se configurar o spi, o tipo de hash e a palavra do hash.

Tabela 59: Comandos para configuração da autenticação por área, RFC 4552 no OSPFv3

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ipv6 router ospf	Acessa o modo de configuração do protocolo OSPFv3.
4	CPE(config-ospfv6)# area area authentication ipsec spi num [sha1 | md5] hashkey	Habilita o modo ipsec AH de autenticação. Deve-se configurar o spi, o tipo de hash e a palavra do hash

Tabela 60: Comandos para configuração da autenticação por interface, RFC 6506 no OSPFv3

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface iface num	Acessa a interface que se deseja fazer a autenticação.
4	CPE(config-ifacenum)# ipv6 ospf authentiction-trailer-mode [md5 | sha1 | sha256 | sha384 | sha 512]	Habilita o modo trailer mode na autenticação. É necessário definir o tipo de hash desejado.
5	CPE(config-ifacenum)# ipv6 ospf authentiction-trailer-key keyid key	Define a chave de deve usada nas duas pontas

4.8.5. Border Gateway Protocol

O BGP (Border Gateway Protocol) (RFC 4271) permite a troca de informações entre os ASs (Autonomous Systems), que formam a Internet. Dentro dos ASs o roteamento é feito através de um IGP (Interior Gateway Protocol) como por exemplo o RIP e/ou OSPF. Quando dois roteadores que pertencem a um mesmo AS trocam informações sobre rotas, eles executam iBGP (internal BGP). Se os roteadores pertencem a diferentes ASs, diz- se então que eles executam eBGP (external BGP).

Uma descrição breve do funcionamento deste protocolo é feita a seguir:

- Primeiramente é estabelecida uma conexão TCP entre os dois roteadores (os neighbors ou peers BGP), que trocam mensagens de abertura da sessão (open) e negociam os parâmetros de operação;
- Os peers trocam tabelas completas de rotas BGP. Após, são enviadas apenas as atualizações das tabelas, quando ocorrem mudanças nas informações de roteamento. Durante uma sessão, os roteadores armazenam a informação de versão da tabela BGP, que é a mesma para todos os peers. Se houver interrupção na sessão por qualquer motivo, o processo é reiniciado.
- Nos intervalos entre as mensagens update são enviadas mensagens de keepalive;
- São enviadas mensagens de aviso quando ocorrem erros ou outras situações especiais;
- Se for verificado erro em uma conexão, uma mensagem é enviada e a conexão fechada.

O BGPv4 é compatível com a RFC4273 para MIB. O OID para o ospf v2 é 1.3.6.1.2.1.15 de acordo com a BGP4-MIB. Também há opção de ligar as traps do BGP.

4.8.5.1. Configurações do BGP

Os procedimentos para configuração de funcionalidades básicas do BGP são apresentados na tabela abaixo.

Tabela 61: Configurações básicas do protocolo BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number **Exemplo:** CPE (config)# router bgp 200	uração do roteador BGP. O parâmetro as-number deve ter or BGP usa-se: **no router bgp as-number**
4	CPE (config-bgp)# [no] network netw-addr/mask	Define as redes que serão anunciadas via BGP ou remove uma rede previamente configurada.
5	CPE (config-bgp)# [no] neighbor neighbor-addr remote-as as-number	No BGP é necessário definir as adjacências através do comando **neighbor**, uma vez que os roteadores não descobrem seus vizinhos de forma automática. Existem dois tipos de vizinhança: interna (quando os roteadores pertencem a um mesmo AS) e externa (entre equipamentos que estão em diferentes ASs). No primeiro caso, os roteadores podem estar em qualquer lugar do AS, enquanto que no segundo caso geralmente existe adjacência. A vizinhança deve ser configurada nas duas pontas. Para remover um neighbor, usa-se o **no** a frente do comando.
6	CPE (config-bgp)# neighbor neighbor-addr description text	(Opcional) Insere uma descrição do neighbor. Para remover uma descrição usa-se: **no neighbor neighbor-addr description**
7	CPE (config-bgp)# neighbor neighbor-addr maximum-prefix prefix-limit [threshold] [restart interval] [warning-only]	(Opcional) Este comando limita o número de prefixos recebidos de um determinado neighbor que devem ser aceitos. **Parâmetros:** **prefix-limit:** Quantidade máxima de prefixos aceitos, de 1 até 4294967295. **threshold:** percentual no qual deve ser gerada uma advertência relacionada ao limite de prefixos (de 1 até 100). **warning-only:** Apenas gera uma advertência quando o limite de prefixos é excedido. **restart interval:** Intervalo em minutos, de 1 até 65535. Para remover a limitação de prefixos usa-se: **no neighbor neighbor-addr maximum-prefix**

8	CPE (config-bgp)# neighbor neighbor-addr remove-private-as	(Opcional) Remove os números de AS privados das atualizações. A faixa de ASs privados é de 64512 até 65534. Esta configuração é válida para vizinhos externos ao AS (eBGP) e nunca remove números de AS públicos. Este comando deve ser usado sempre que forem empregados números de ASs privados. Quando uma rede possui apenas uma conexão para upstream (caso em que o cliente adquire trânsito de um provedor), as políticas de roteamento tendem a ser as mesmas utilizadas pelo provedor de serviço e normalmente não existe a necessidade de utilizar um número distinto de AS neste tipo de rede. Ainda que a rede faça uso do BGP para upstream, o domínio pode empregar um número de AS da faixa privada (64512 até 65534) nas seções BGP com o provedor. Neste caso o número de AS privado é retirado dos anúncios que serão reenviados e o ASN do provedor aparece como sendo o AS de origem do tráfego. Se um AS possui conexões de downstream (comercialização de trânsito), ainda assim é possível que o mesmo utilize números de AS privados. Porém, se um AS possui mais de uma conexão para upstream, este deve utilizar um número de AS único. Para remover esta configuração, usa-se: **no neighbor neighbor-addr remove-private-as**
	CPE (config-bgp)# [no] network netw-addr/mask backdoor	(Opcional) É possível que um roteador receba atualizações sobre uma mesma rede através do protocolo BGP e de um IGP (como OSPF ou RIP). Neste caso, devido ao fato de a distância administrativa do BGP ser menor do que as distâncias dos IGPs, o roteador prefere alcançar a rede através da rota aprendida via BGP. O comando **backdoor** faz com que a rota aprendida via um IGP seja preferencial. **netw-addr/mask** é a rede a ser alcançada via IGP. O BGP não envia atualizações sobre esta rede. Para remover a configuração backdoor, usa-se o **no** a frente do comando.

A seguir são mostradas algumas configurações avançadas de propósito geral do BGP.

Tabela 62: Configurações avançadas do protocolo BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# [no] neighbor neighbor-addr advertisement-interval interval	(Opcional) Define o intervalo mínimo para envio de atualizações sobre rotas, de 0 até 600 segundos. Para remover um intervalo configurado usa-se: **no neighbor neighbor-addr advertisement-interval**.
4	CPE (config-bgp)# neighbor neighbor-addr shutdown	(Opcional) Desabilita um neighbor sem remover a configuração relacionada a ele. Para reabilitá-lo, usa-se: **no neighbor neighbor-addr shutdown**
4	CPE (config-bgp)# neighbor neighbor-addr passive	(Opcional) Define que não serão enviadas mensagens open para este vizinho. Para remover esta configuração usa-se: **neighbor neighbor-addr passive**
4	CPE (config-bgp)# neighbor neighbor-addr password password	(Opcional) Habilita o uso de autenticação MD5 nas conexões TCP para o neighbor especificado. Para desabilitar a autenticação usa-se: **no neighbor neighbor-addr password**
4	CPE (config-bgp)# neighbor neighbor-addr port tcp-port	(Opcional) Configura a porta TCP do neighbor. A porta default do BGP é a 179.
4	CPE (config-bgp)# neighbor neighbor-addr timers {keepalive-interval holdtime | connect connect-timer}	(Opcional) Ajusta os timers do BGP para o neighbor especificado. Os valores devem ser de 0 até 65535 segundos. Para remover esta configuração usa-se: **no neighbor neighbor-addr timers [connect]**
4	CPE (config-bgp)# neighbor neighbor-addr update-source{interface | addr}	(Opcional) O uso de interfaces loopback para definir neighbors é bastante comum em iBGP e normalmente tem como objetivo garantir que o endereço IP configurado estará sempre ativo. Porém, para utilizar o endereço da interface loopback no comando **neighbor** em um roteador é necessário informar ao BGP que executa no roteador que este deve iniciar a conexão TCP com o neighbor fazendo uso do endereço da loopback. Isto é feito através do comando **neighbor upadate-source**.
4	CPE (config-bgp)# neighbor neighbor-addr peer-group word	(Opcional) Definir um peer-groups no BGP simplifica as configurações do protocolo e traz como benefício a redução das quantidades de processamento e memória necessária para a geração de atualizações, uma vez que a tabela de roteamento é verificada somente uma vez e é replicada para todos os membros do peer-group, ao invés de ser verificada para cada peer. Para remover esta configuração usa-se: **no neighbor neighbor-addr peer-group word**

4.8.7.1. Multiprotocol BGP

O protocolo BGP, conforme sua especificação original (RFC4271), foi projetado para transportar apenas rotas IPv4. Isso é evidente quando se analisa o formato da mensagem BGP UPDATE, onde determinados campos são codificados implicitamente como um prefixo ou uma lista de prefixos IPv4. Com o propósito de contornar essa restrição, a RFC2858 extende o BGP adicionando a capacidade de transportar rotas de múltiplos protocolos de camada de rede. Essas extensões são conhecidas como extensões multi-protocolo e são utilizadas, por exemplo, para permitir o roteamento inter-domínio para IPv6. A tabela abaixo mostra os comandos para configuração das extensões multiprotocolo do BGP.

Tabela 63: Configuração das extensões multiprotocolo do BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE(config-bgp)# address-family ipv6 unicast	Entra no modo de configuração para a adress-family IPv6.
5	CPE(config-bgp-af)# neighbor *neighbor-addr* activate	Habilita as extensões multi-protocolo para a troca de prefixos IPv6 para o neighbor especificado.

4.8.7.2. RouteReflectors

O uso de Route Reflectors (RRs) no BGP consiste em uma solução para prevenir o aumento excessivo da quantidade de sessões BGP dentro de um AS. Um roteador BGP não deve anunciar uma rota que ele aprendeu via BGP de outro roteador iBGP para terceiro roteador iBGP. Esta restrição pode ser relaxada a fim de permitir que um roteador anuncie ou reflita rotas aprendidas via iBGP para outros roteadores iBGP. Esta abordagem reduz o número de pares iBGP dentro de um AS.

É necessário eleger um roteador para exercer o papel de route reflector, enquanto que os outros irão atuar como clientes deste (route reflector clients). Ainda podem existir roteadores que atuam em modo convencional (non clients), cuja configuração é feita normalmente com o comando **neighbor.** Para os clientes e não-clientes a existência de route reflectors é transparente. A tabela abaixo mostra os comandos para a configuração de route reflectors.

Tabela 64: Configuração de route reflectors

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# neighbor neighbor-addr route-reflector-client	(Opcional) Este comando deve ser executado no route reflector para cada neighbor cliente. A combinação de um RR e seus clientes é chamada de cluster.
5	CPE (config-bgp)# bgp cluster-id id	(Opcional) Normalmente um cluster contém um único RR, sendo o cluster identificado pelo id do RR neste caso. Porém, mais RR podem ser adicionados ao cluster com o objetivo de prover redundância. Neste caso deve ser configurado um identificador que deve ser comum a todos os RRs de um cluster. Para tanto, deve ser usado o comando **bgp cluster-id**, sendo o cluster-id um valor de 1 até 4294967295 ou ainda, sob a forma de endereço IP.

4.8.7.3. Autonomous System Confederations for BGP

O uso de confederações BGP é outra forma de controlar o aumento excessivo de sessões BGP dentro de um AS. Essa técnica é baseada na idéia de que um AS pode ser dividido em múltiplos sub-AS's. Dentro de cada sub-AS todas as regras do iBGP são aplicadas. Para o roteamento entre sub-AS's diferentes, o eBGP é utilizado. Apesar de o eBGP ser utilizado entre sub-AS's diferentes, os atributos NEXT_HOP, MED e LOCAL PREFERENCE são preservados no roteamento entre esses sub-AS's. Para o mundo externo, uma confederação BGP composta de múltiplos sub-AS's aparenta ser um único AS. A tabela abaixo mostra os comandos para a configuração de *confederações BGP*.

Tabela 65: Configuração de BGP confederations

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE(config-bgp)# bgp confederation identifier as-number	Configura o identificador da confederação BGP.
5	CPE (config-bgp)# bgp confederation peers as-number [... as-number]	Configura os sistemas autônomos que fazem parte da mesma conferação BGP que o roteador.

4.8.7.4. BGP Multipath

Quando um roteador aprende duas rotas eBGP idênticas de um AS vizinho, ele vai escolher aquela com menor id como sendo a melhor rota, instalando a mesma na sua tabela de roteamento. Porém, se o suporte a BGP multipath é ativado, diversas rotas são instalados na tabela de roteamento (ao invés de uma). Durante a comutação de pacotes, o balanceamento de carga pode ser realizado por destino, entre as várias rotas disponíveis. A tabela abaixo mostra os comandos para configuração de BGP multipath.

Tabela 66: Configuração de BGP multipath

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# maximum-pathsvalue **Exemplo:** CPE (config-bgp)# maximum-paths4	(Opcional) Este comandocontrola o número máximo de rotas suportadas. No exemplo o BGP é configurado para suportar até 4 melhores rotas para balanceamento de carga. Para remover a configuração usa-se: **no maximum-paths**

4.8.7.5. BGP Multihop

Os peers eBGP normalmente estão em redes diretamente conectadas. Para os casos em que não é possível manter esta condição, usa-se o comando **neighbor ebgp-multihop**, conforme mostra a tabela abaixo.

Tabela 67: Configuração de eBGP multihop

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# neighbor neighbor-addr ebgp-multihop [maximum-hop-count]	(Opcional) Este comando é usado para indicar que o neighbor eBGP não está diretamente conectado ao roteador local. **Importante:** Deve-se garantir que o neighbor indicado é alcançável pelo roteador local, por exemplo, através de uma rota estática. A opção **maximum-hop-count** indica o número máximo de saltos necessários para alcançar o neighbor especificado. Para remover a configuração usa-se: **no neighbor neighbor-addr ebgp-multihop [maximum-hop-count]**

4.8.7.6. Graceful Restart para BGP

Quando o BGP de um roteador é reinicializado, normalmente os seus vizinhos BGP detectam que uma de suas sessões caiu e depois que ela voltou. Essas transições fazem com que todos esses vizinhos recalculem suas tabelas de roteamento e podem também gerar um efeito cascata onde o mesmo processo se repete em vários domínios vizinhos. Esse comportamento não é adequado em casos onde essas transições não refletem mudanças na topologia, mas apenas uma reinicialiação do plano de controle de um roteador. Para evitar mudanças bruscas e desnecessárias no plano de dados de roteadores que usam o BGP, foi criada a extensão Graceful Restart, onde o plano de dados dos roteadores BGP permanece inctacto enquanto um processo BGP é reinicializado. A tabela abaixo mostra os comandos para a configuração do BGP graceful restart.

Tabela 68: Configuração de BGP graceful restart

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE(config-bgp)# bgp graceful-restart [stalepath-time seconds]	Habilita o graceful restart para o BGP. Ao configurar esse comando, é necessário que o BGP seja reiniciado caso alguma sessão BGP já tenha sido estabelecida. Isso é necessário para que essa capacidade seja anunciada para todos os neighbors.

4.8.7.7. Filtragem de rotas BGP com access lists

No protocolo BGP é possível restringir as informações de roteamento que são enviadas para um neighbor ou peer-group específico ou recebidas através do uso de access lists. Os comandos para a configuração e aplicação de access lists no BGP são apresentados na tabela abaixo.

Tabela 69: Uso de access lists no BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# neighbor {neighbor-addr | peer-group-name} distribute-list access-list-number {in | out} **Exemplo:** Evitar a propagação de uma rede específica com uso de ACL padrão: CPE (config)# access-list 10 deny 192.10.1.0 0.0.0.255 CPE (config)# access-list 1 permit 0.0.0.0 255.255.255.255 CPE (config-bgp)# router bgp 100 CPE (config-bgp)# neighbor 3.3.3.3 remote-as 300 CPE (config-bgp)# neighbor 2.2.2.2 remote-as 200 CPE (config-bgp)# neighbor 2.2.2.2 distribute-list 10 out	(Opcional) Para restringir o envio ou recebimento de informações de roteamento de ou para um neighbor ou peer-group específico é necessário definir uma access list e aplicá-la com o comando **distribute-list**no modo de configuração do BGP. No exemplo tem-se dois neighbors, dos ASs 200 e 300. Para o AS 300 não há nenhuma restrição quanto ao envio de atualizações sobre rotas, enquanto que para o AS 200 são filtradas as atualizações da rede 192.10.1.0/24, sendo permitidas todas as outras redes. **Importante:** Na configuração de wild cards, o bit **0** indica a necessidade de correspondência exata, enquanto que o bit **1** não é verificado. (No exemplo 1, **255.255.255.255** indica que todas as redes são permitidas).

4.8.7.8. Filtragem de rotas BGP com prefix-lists

As prefix lists podem ser utilizadas no BGP como alternativa às access lists para filtrar as atualizações enviadas ou recebidas com base no prefixo. Porém, os comandos **neighbor prefix-list** e **neighbor distribute-list** não devem sob hipótese alguma serem aplicados em um mesmo neighbor e em um dado sentido. Em outras palavras, não é possível configurar para um mesmo neighbor os comandos **neighbor a.b.c.d prefix-list list1 in** e **neighbor a.b.c.d distribute-list list2 in**.

Tabela 70: Configuração de prefix-lists no BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config)# ip prefix-listlist-name [seq seq-number] {deny | permit} netw-addr/mask [ge value] [le le value] CPE (config-bgp)# neighbor neighbor-addr prefix-list word {in | out} **Exemplo:** CPE (config)# ip prefix-list list_as200 deny 183.0.0.0/8 ge 24 le 32 CPE (config-bgp)# router bgp 100 CPE (config-bgp)# neighbor neighbor-addr prefix-list list_as200 out	(Opcional) O comando **ip prefix-list** cria uma prefix list. As prefix-lists são analisadas de cima para baixo e o processamento das mesmas é encerrado no momento em que o pacote que é verificado atende ao critério especificado em uma linha. Uma lista vazia permite todo todos os prefixos e ao final de uma lista não vazia tem- se implícita a linha **deny any**. Para aplicar uma prefix-list usa-se o comando **neighbor prefix-list**. **Opções:** **seq:** É o número de sequência e pode ser setado de modo manual ou automático. No modo manual, devem ser utilizados valores de 1 a 9999999, enquanto que no modo automático este número será incrementado de 10 a cada entrada da lista. Se uma lista é criada sem o seq-number após uma lista com o seq-number especificado, a nova lista assume como seq-number o próximo múltiplo de 10. **Operadores:** **le:** A prefix-list será aplicada se a máscara é menor que ou igual ao valor especificado após le. **ge:** A prefix-list será aplicada se máscara é maior que ou igual ao valor especificado após ge. No exemplo, são negados todos os prefixos **/24** até **/32** para o endereço de rede 183.0.0.0/8.

Comandos relacionados

A tabela abaixo mostra os comandos para verificação das prefix-lists configuradas.

Tabela 71: Verificação de prefix-lists no BGP

CPE# show ip prefix-list [detail | summary]	Exibe informações sobre as prefix lists configuradas.
CPE# show ip prefix-list [detail | summary] prefix-list-name	Exibe informações sobre uma prefix lists específica.
CPE# show ip prefix-listprefix-list-name [netw-addr/mask]	Exibe informações sobre a política associada a rede especificada.
CPE# show ip prefix-list prefix-list-name [seq seq-number]	Exibe as informações da entrada da prefix list especificada com o seq-number.
CPE# show ip prefix-list prefix-list-name [netw-addr/mask] longer	Exibe as entradas da prefix list que são mais específicas do que a rede e máscara fornecidas.
CPE# show ip prefix-list prefix-list-name [netw-addr/mask] first-match	Exibe a entrada da prefix list que corresponde a rede e a máscara fornecidas.

4.8.7.9. Uso de route maps no BGP

Os route maps assemelham-se aos comandos condicionais se...então... utilizados nas linguagens de programação. Existem diversas aplicações para os route maps, estando entre as mais comuns a filtragem de rotas durante a redistribuição nos protocolos de roteamento (não somente no BGP) e a modificação de atributos nos vizinhos BGP. A tabela abaixo mostra os passos necessários para configurar route-maps para controle de rotas a serem propagadas.

Tabela 72: Configuração de route-maps no BGP para restringir a propagação de rotas

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# access-list acl-number {permit | deny} netw-addr wild-card	Configura uma ACL para ser verificada durante a execução do route-map.
	CPE (config)# route-map word {permit | deny} seq-number	Configura o route map atribuindo um número de sequencia ao mesmo (seq-number). O route-map com menor seq-number é executado primeiro. **Importante:** Deixar espaço entre os seq-numbers facilita a realização de atualizações ou modificações futuras. Ao final de um route-map tem-se a seguinte linha implícita: **route-map word deny 65536** Esta linha faz com que todas as redes que não corresponderem a nenhuma entrada do route map sejam negadas.
4	CPE (config-route-map)# match ip {address | next-hop | route-source} {acl-number | prefix-list-name}	As declarações **match** são usadas para chamar as access lists e podem ou não ser seguidas de declarações **set**. **Importante:** Para evitar que o route-map se aplique a todos os pacotes é fundamental o uso do comando **match.** Este comando filtra uma rota com base no endereço IP da rede, da fonte ou do next-hop, que devem ser previamente configurados em uma ACL ou prefix list.
5	CPE (config-route-map)# exit	Deixa o modo de configuração do route-map.

6	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
7	CPE (config-bgp)# neighbor neighbor-addr route-map word {in | out} **Exemplo:** CPE (config)# access-list 1 permit 172.1.0.0 0.0.0.255 CPE (config)# access-list 11 permit 0.0.0.0 255.255.255.255 CPE (config)# route-map UPDATES_AS200 deny 10 CPE (config-route-map)# match ip address 1 CPE (config-route-map)# exit CPE (config)# route-map UPDATES_AS200 permit 20 CPE (config-route-map)# match ip address 11 CPE (config)# router bgp 100 CPE (config-bgp)# neighbor2.2.2.2remote-as 200 CPE (config-bgp)# neighbor2.2.2.2route-map UPDATES_AS200out	(Opcional) Este comando faz com que route-map atue como um filtro, podendo negar ou propagar rotas com base em diferentes critérios. No exemplo tem-se uma ACL que permite a rede 172.1.0.0/24 e (de forma implícita) nega todo o restante do tráfego. O comando **route-map UPDATES_AS200 deny 10** e a linha **match ip address 1** fazem com que a rede 172.1.0.0/24, que é referenciada na ACL 1 seja negada. O número de sequência 10 faz com que essa entrada do route map seja executada primeiro. As redes que não correspondem ao que foi especificado na ACL 1 serão analisadas na entrada com número de sequência 20 do route map, que permite as redes que correspondem a ACL 11 (onde todo o tráfego é permitido). O comando neighbor2.2.2.2**route-map UPDATES_AS200** faz com que todas as rotas a serem propagadas para o roteador 2.2.2.2 sejam verificadas segundo os critérios descritos acima.
8	CPE (config-bgp)# network netw-addr/mask route-map word	(Opcional) O uso do comando route-map junto ao comando network tem como objetivo modificar os atributos dos prefixos que combinam com o que foi especificado pelo comando **network**.

A tabela a seguir apresenta os comandos para configuração de route maps modificação de atributos do BGP.

Tabela 73: Configuração de route-maps no BGP para modificação de atributos

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# access-list acl-number {permit | deny} netw-addr wild-card	Configura uma ACL para ser verificada durante a execução do route-map.
4	CPE (config)# route-map word {permit | deny} seq-number	Configura o route map atribuindo um número de sequencia ao mesmo (seq-number). O route-map com menor seq-number é executado primeiro. **Importante:** Deixar espaço entre os seq-numbers facilita a realização de atualizações ou modificações futuras.
5	CPE (config-route-map)# match aspath word	As declarações **match** são usadas para chamar as access lists e podem ou não ser seguidas de declarações **set**. **Importante:** Para evitar que o route-map se aplique a todos os pacotes é fundamental o uso do comando **match.** Este comando verifica se uma rota possui o AS PATH especificado. Sempre que uma atualização de rota passa através de um AS, o número deste AS passa a constar nessa atualização. Assim, o atributo AS_PATH indica a listagem ASs que uma rota atravessou a fim de alcançar um destino.
5	CPE (config-route-map)# match metric metric	Verifica se uma rotapossui a métrica (MED) especificada. O atributo métrica (ou MED, de Multi Exit Discriminator) indica para os neighbors externos ao AS local as rotas que são preferenciais para alcançar um AS especificado quando existem múltiplos pontos de entrada para o mesmo. O valor mais baixo é o preferido.
5	CPE (config-route-map)# match community community-list	Verifica uma rota de acordo com a community list especificada. O atributo community é um atributo é opcional e agrupa destinos em uma determinada comunidade, podendo serem aplicadas decisões de roteamento de acordo com essas comunidades.

5	CPE (config-route-map)# match extcommunity {acl-number | word}	Verifica uma rota de acordo com a extended community list BGP/VPN. Este atributo é utilizado com a tecnologia MPLS VPN / BGP, sendo bastante similar ao atributo community.
5	CPE (config-route-map)# match origin {egp | igp | incomplete}	Verifica a origem da rota. Este atributo define a origem das informações sobre uma determinada rota. **Opções:** **igp:** Interior ao AS. **egp:** Exterior ao AS. **Incomplete:** É desconhecida ou aprendida através de outros meios.
5	CPE (config-route-map)# match peer {peer-addr | local}	Verifica o peer que divulgou a rota.
6	CPE (config-route-map)# set aggregator as as-number aggregator-addr	Modifica o atributo aggregator do BGP. Este atributo é opcional, podendo ser incluído nas atualizações de rotas que são formadas por agregação. O aggregator deve conter o seu número de AS e o identificador BGP.
	CPE (config-route-map)# set as-path {exclude | prepend} as-path	Modifica o atributo AS PATH.
	CPE (config-route-map)# set atomic-aggregate	Modifica o atributo atomic aggregate do BGP. Este atributo indica que o roteador realizou a agregação de rotas.
	CPE (config-route-map)# set comm-list {acl-number | acl-name} delete	Modifica o atributo community list do BGP.
	CPE (config-route-map)# set community {aa:nn | none} [no-export | no-advertise | internet | additive]	Modifica o atributo community list do BGP. **Opções:** **no-export:** A rota não deve ser anunciada para nenhum neighbor externo ao AS. **no-advertise:** A rota não deve ser anunciada para nenhum neighbor, interno ou externo. **internet:** A rota deve ser anunciada para todos os neighbors.
	CPE (config-route-map)# set extcommunity {rt | soo}? as:nn	Modifica o atributo extended community do BGP. **Opções:** **rt:**Route Target extended community **soo:**Site-of-Origin extended community
	CPE (config-route-map)# set ip next-hop {next-hop-addr | peer-address}	Modifica o atributo next hop do BGP.
	CPE (config-route-map)# set local-preference preference	Modifica o atributo local preference do BGP. O atributo local preference é uma indicação para o AS que caminho é o preferido para atingir uma determinada rede. Quando há vários caminhos para o mesmo destino, o caminho com a maior preferência é o escolhido. O valor padrão deste atributo é 100.

	CPE (config-route-map)# set origin {egp | igp | incomplete}	Modifica o atributo origin.
	CPE (config-route-map)# set originator-id originator-addr	Modifica o atributo originator ID. Este atributo é utilizado pelos route reflectors com o objetivo de evitar a ocorrência de loops nos ASs que fazem uso deste recurso.
	CPE (config-route-map)# set vpnv4 next-hop next-hop-addr	Modifica o atributo VPNv4 next hop.
	CPE (config-route-map)# set weight weight	Modifica o atributo weight do BGP. O valor do atributo weight é definido localmente para o roteador e só tem sentido para o roteador específico, não sendo enviado nas atualizações de rota. O weight pode ser um número de 0 a 65.535, sendo que as rotas que são originadas no roteador local assumem valor 32.768 para este atributo por padrão, enquanto que as demais tem valor 0.
7	CPE (config-route-map)# exit	Deixa o modo de configuração do route-map.
8	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
9	CPE (config-bgp)# neighbor neighbor-addr route-map word {in | out} **Exemplo:** CPE (config)# route-map UPDATES_AS400 permit 20 CPE (config-route-map)# set local-preference 5000 CPE (config-route-map)# set weight 1000 CPE (config-route-map)# exit CPE (config)# router bgp 100 CPE (config-bgp)# neighbor4.4.4.4remote-as 400 CPE (config-bgp)# neighbor4.4.4.4route-map UPDATES_AS400in	(Opcional) Este comando faz com que route-map atue como um filtro, podendo negar ou propagar rotas com base em diferentes critérios. No exemplo não foi configurado nenhum **match**,fazendo com que as declarações **set** sejam aplicadas a todas as atualizações recebidas do neighbor 4.4.4.4. Neste caso, o atributo local preference passa a ter valor 5000 e o atributo weight assume valor 1000.

Comandos relacionados

CPE# show ip bgp route-map word	Exibe informações relacionadas ao route map especificado.

4.8.7.10. BGP Route Servers

A fim de trocar tráfego, dois provedores de serviço podem se conectar de duas formas: através de peering público ou privado.

No peering privado, os provedores definem como as suas redes serão conectadas mantém um contrato com todos os detalhes da conexão. Além disso, eles disponibilizam o espaço físico e os equipamentos necessários para a operação.

Já no peering público, existe uma estrutura compartilhada entre os provedores, chamada de ponto de troca de tráfego (PTT). Um PTT é formado fisicamente por um conjunto de roteadores localizados em um único ponto neutro, conectados através de um switch e formando uma rede local de alta velocidade. Cada roteador pertence a um sistema autônomo que deseja trocar tráfego com pelo menos um dos participantes.

Normalmente as conexões eBGP entre estes roteadores são feitas pelo método full-mesh, o que tende a apresentar problemas de escalabilidade devido ao grande número de conexões que deve ser mantido por cada peer. Neste aspecto, o uso de um BGP route server possibilita que cada peer esteja conectado somente ao route server.

Diferentemente de um roteador BGP convencional, o BGP route server deve gerenciar diversas políticas de roteamento para cada um de seus peers. É possível que um roteador BGP atue como route server e como roteador convencional ao mesmo tempo.

A tabela abaixo mostra como configurar um route-server.

Tabela 74: Configuração de route servers BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# neighbor neighbor-addr route-server-client	Configura um neighbor como cliente. Nenhum atributo BGP que é repassado ao neighbor especificado deve ser modificado.
5	CPE (config-bgp)# neighbor neighbor-addr route-map word {import | export}	Configura o uso de um route-map que define a política de exportação ou importação de informações de roteamento do peer que foi configurado como route server client no comando anterior. **Importante:** Para configurar um route-map consulte a seção**"Uso de route maps no BGP".**

4.8.7.11. Agregação de rotas no BGP

Agregação é o processo que combina as características de várias rotas diferentes de forma que a propagação de uma única rota seja possível, a fim de minimizar o tamanho das tabelas de roteamento. A tabela a seguir mostra os comandos relacionados a agregação de rotas no BGP.

Tabela 75: Comandos para agregação de rotas no BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# aggregate-address addr mask **Exemplo:** CPE (config-bgp)# aggregate-address 172.0.0.0 255.0.0.0	(Opcional) Este comando faz com que seja anunciada a rota configurada além de todas as rotas mais específicas. No exemplo, o comando **aggregate-address** faz com que seja propagada a rede 172.0.0.0 e todas as redes mais específicas que tenham sido aprendidas, como por exemplo 172.1.1.0. **Importante: Este comando deve ser usado somente para um endereço do qual se tem uma rota mais específica na tabela de roteamento do BGP.**
	CPE (config-bgp)# aggregate-address addr mask [summary-only] [as-set] **Exemplos:** 1) CPE (config-bgp)# aggregate-address 172.0.0.0 255.0.0.0 summary-only CPE (config-bgp)# aggregate-address 172.0.0.0 255.0.0.0 as-set	(Opcional) A opção **summary-only** faz com que as rotas mais específicas sejam suprimidas e somente a rota indicada seja propagada. No exemplo 1, se o roteador tiver em sua tabela BGP as redes 172.1.0.0 e172.20.2.0, somente a rede 172.0.0.0 será propagada. A opção **as-set** faz com que sejam incluídas informações sobre os ASs através do quais as rotas sumarizadas passaram o que contribui para que sejam evitados loops no roteamento.

Outros comandos

Sempre que ocorrem mudanças nas configurações do BGP, as sessões necessitam ser reiniciadas para que tais mudanças tenham efeito. Contudo, reiniciar uma sessão consome boa quantidade de processamento e memória e causa impacto no funcionamento das redes. A tabela a seguir mostra os comandos para remover informações de roteamento do BGP.

Tabela 76: Comandos para remover informações de roteamento no BGP

Comando	Objetivo
CPE (config-bgp)# neighbor neighbor-addr soft-reconfiguration inbound	Define o uso de soft reconfiguration para o neighbor especificado, a fim de permitir que novas configurações tenham efeito sem que seja necessário reiniciar as sessões BGP, por meio do armazenamento de uma cópia das informações de roteamento recebidas do neighbor especificado
CPE# clear ip bgp *	Reinicia todas as conexões BGP.
CPE# clear ip bgp as-number neighbor-addr | peer-group peer-group-name [in prefix-filter]	Reinicia a sessão com o neighbor ou peer-group especificado.
CPE# clear ip bgp {as-number neighbor-addr | neighbor-addr } out	Reinicia a sessão com o neighbor especificado.
CPE# clear ip bgp {as-number neighbor-addr | neighbor-addr | peer-group peer-group-name}ipv4 {unicast | multicast} {in prefix-filter | out | soft {in | out}}	Reinicia as sessão BGP IPv4, unicast ou multicast para o neighbor ou peer-group especificado. **Parâmetros:** **soft in:** Tem efeito sobre as atualizações recebidas de um neighbor. **soft out:** Tem efeito sobre as atualizações que são enviadas para um neighbor.
CPE# clear ip bgp {as-number neighbor-addr | neighbor-addr}rsclient | soft {in | out}	Reconfigura o neighbor especificado, que é um cliente do route server. **Parâmetros:** **rsclient:** route server client **soft in:** Tem efeito sobre as atualizações recebidas de um neighbor. **soft out:** Tem efeito sobre as atualizações que são enviadas para um neighbor.
CPE# clear ip bgp peer-group peer-group-name rsclient	Reconfigura o peer group especificado, no qual os participantes são clientes do route server.
CPE# clear ip bgp {as-number neighbor-addr | neighbor-addr}vpnv4 [unicast in | unicast out | unicast soft in | unicast soft out]	Reinicia as sessões VPNv4, unicast ou multicast, com ou sem soft reconfiguration.
CPE# clear ip bgp external {in [prefix-filter] | out}	Reinicia as sessões de eBGP.
CPE# clear ip bgp external ipv4 {unicast | multicast} {in prefix-filter | out | soft {in | out}}	Reinicia as sessões eBGP IPv4, unicast ou multicast.

	O mecanismo conhecido como **route refresh capability** constitui uma outra solução para o problema causado quando as seções BGP são reiniciadas. Esta funcionalidade permite que o roteador local envie mensagens requisitando uma cópia da RIB que é enviada por este peer. Os peers que tem esta funcionalidade habilitada anunciam a mesma durante o estabelecimento da sessão BGP (com uso do BGP Capabilities advertisement). Quando são feitas mudanças na política de roteamento de entrada, o roteador local envia uma requisição de atualização, pedindo ao peer que anuncie novamente as suas atualizações.
CPE# clear ip bgp dampeningnetw-addr/mask	Este comando limpa as informações relacionadas ao route-dampening. O route dampening é uma funcionalidade do BGP que foi projetada para minimizar a propagação de rotas cuja disponibilidade se alterna repetidamente.

4.8.7.12. Configuração de BFD no BGP

A tabela abaixo mostra os comandos para configuração do BFD (Bidirectional Forwarding Detection) no BGP.

Tabela 77: Comandos para configuração do BFD no BGP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# router bgp as-number	Acessa o modo de configuração do roteador BGP.
4	CPE (config-bgp)# neighbor neighbor-addr fall-over bfd	(Opcional) Habilita a detecção de falhas através do BFD. **Importante:** É fundamental configurar os timers do BFD conforme consta na seção **"Bidirectional Forwarding Detection – BFD"**.

Comandos Relacionados

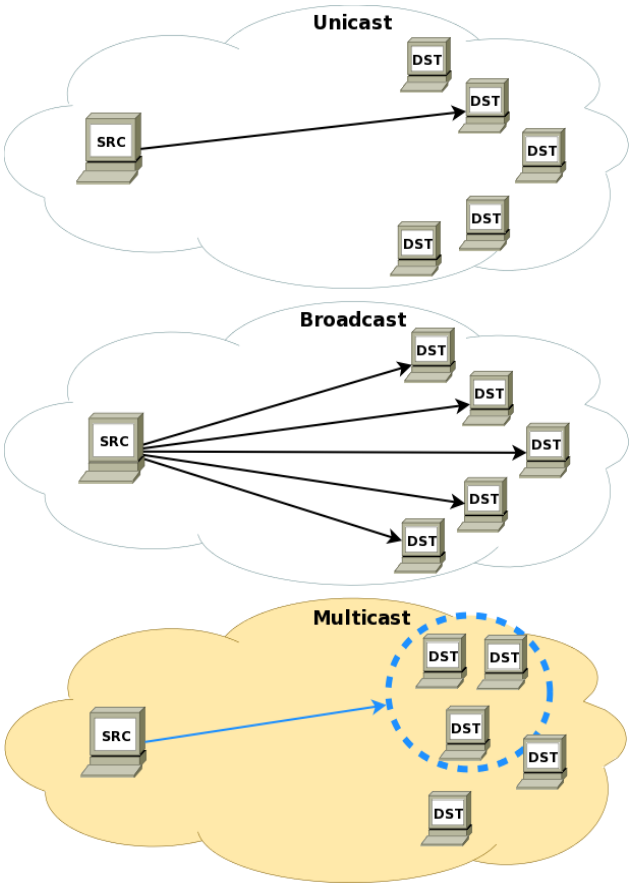
CPE# show bfd neighbors	Exibe informações sobre os neighbors BFD, tais como endereço IP, quantidade de pacotes recebidos e enviados, e estado (up/down).

4.8.8. IP Multicast

IP Multicast é uma tecnologia que reduz o tráfego da rede ao permitir que se entregue apenas um fluxo de informação a mais de um receptor. Vídeo conferência, vídeo, áudio e distribuição de notícias são exemplos de aplicações que podem se beneficiar desta tecnologia.

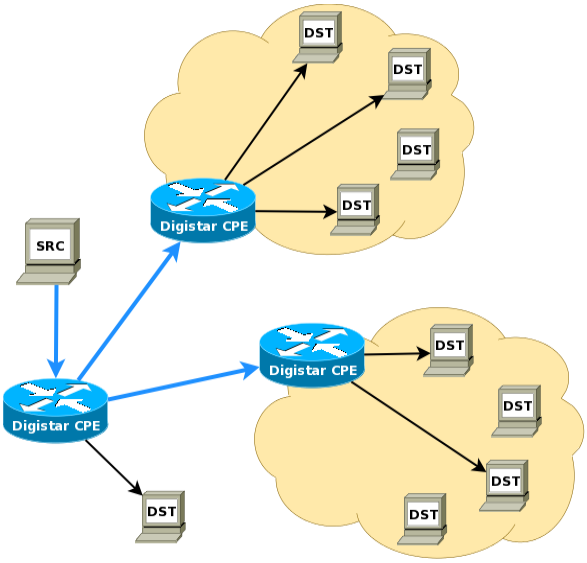
Ela permite que um host (fonte) envie informação para um grupo de hosts (receptores) através de um endereço IP Multicast. Os endereços IPv4 atribuídos pela IANA para o uso em multicast compreende a faixa do IP 224.0.0.0 até o 239.255.255.255. A fonte envia informação para um endereço de destino desta faixa e roteadores se encarregam de entregar esta informação apenas para hosts que a solicitaram. O conjunto de hosts que solicitaram o recebimento da informação é denominado um grupo multicast. A princípio, qualquer host pode enviar mensagens para um grupo, mas apenas membros do grupo a recebem.

Para entender melhor o que é IP Multicast, observe a figura abaixo. No primeiro exemplo é mostrado o endereçamento unicast: uma fonte envia uma mensagem para apenas um receptor. No segundo exemplo podemos ver o endereçamento broadcast: todos os hosts da rede recebem a mensagem. No último exemplo, é mostrado o endereçamento multicast: apenas um grupo de hosts recebe a mensagem, um grupo multicast.



IP Multicast está, portanto intimamente ligado ao conceito de grupos. Um grupo multicast contém um número arbitrário de receptores que ingressaram nele. O controle destes grupos é feito pelo protocolo IGMP (RFC 2236). É através de mensagens IGMP que hosts pedem para entrar ou sair de grupos. Estas mensagens são de interesse dos roteadores de seus domínios.

Como mostrado na figura abaixo, é papel dos roteadores manterem um controle dos hosts que fazem parte de grupos e replicar a informação apenas no sentido deles, não enviando para os não interessados. Para fazer isso, eles utilizam o protocolo PIM.



4.8.8.1. Modos e Protocolos Suportados

Existem basicamente dois modos de um roteador multicast operar. Estaticamente ou dinamicamente. No modo estático, não há protocolo algum envolvido e as configurações são feitas apenas nos roteadores. Em cada um deve-se configurar os grupos e seus destinos. Neste modo, os hosts não podem ingressar ou deixar grupos quando quiserem, pois a configuração é fixa e feita apenas nos roteadores.

Já no modo dinâmico, são utilizados dois protocolos: um para gerenciamento dos grupos (IGMP), para que hosts possam ingressar e deixar grupos a qualquer momento, notificando seus roteadores, e outro (PIM) utilizado apenas entre roteadores, a fim de resolver o encaminhamento de pacotes multicast.

São suportados os seguintes protocolos para roteamento multicast dinâmico:

- IGMP para o gerenciamento de grupos.
- Protocol Independent Multicast (PIM) entre roteadores multicast. Suportado nos modos Dense Mode, Sparse Mode e Source Specific Mode, brevemente descritos abaixo:
- Dense Mode: o roteador assume que todos outros roteadores queiram encaminhar pacotes multicast. Então encaminha tráfego multicast para todos eles, por padrão, não importando o grupo. Caso algum destes roteadores não tenha hosts interessados em seu domínio, ele envia uma mensagem de volta avisando que não está interessado nos pacotes.
- Sparse Mode: o roteador assume que os outros roteadores não querem encaminhar pacotes multicast a não ser que peçam explicitamente por um grupo.
- Source Specific Mode: semelhante ao Sparse Mode, com a diferença que um grupo é identificado pelo par (Fonte, IP Multicast Destino) e não apenas pelo endereço IP multicast de destino. Isso faz com que os receptores possam solicitar a entrega de mensagens multicast de uma fonte específica. Nos outros dois modos, qualquer host pode mandar mensagens para um grupo, e todos recebem.

4.8.8.2. Configuração de IP Multicast

A configuração de IP Multicast é por interface. É possível que se tenham diferentes configurações operando ao mesmo tempo no roteador, desde que se tenha mais que uma interface. As diferentes combinações funcionam de forma isolada, cada uma sobre um conjunto de interfaces. Por exemplo: configura-se as interfaces ethernet0.10 e ethernet0.20 para o modo estático e as interfaces ethernet1.5 e ethernet1.10 para o modo dinâmico com PIM Sparse Mode.

Ressalta-se que cada interface suporta apenas uma configuração, seja ela manual ou dinâmica. E só é possível ter configurações dinâmicas de um tipo (Dense, Sparse ou Source Specific) para cada interface.

Atenção: diferentes modos funcionam de forma isolada: um pacote que entra por uma interface em Dense mode só poderá sair por uma interface que também opera neste modo, cada modo possui seu conjunto de interfaces.

As configurações dos modos possíveis são mostradas a seguir.

4.8.8.3. Rotas Multicast Manuais

Configura-se para que os pacotes de um determinado grupo sejam replicados em outras interfaces. É necessário que se saiba o endereço IP do grupo multicast, o endereço IP do emissor (fonte) e as interfaces de saída que o conteúdo destinado ao grupo deve ser replicado. Com estas informações, aplica-se o comando uma vez para cada interface de saída.

Tabela 78: Configuração IP Multicast Estático

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface *typenumber* **Exemplo:** *CPE(config)# interface ethernet 1*	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ip mroute group-address *grp-addr* sender-address *src-addr* output-interface {ethernet *num* | tunnel *number*} **Exemplo:** CPE(config-ethernet1)# ip mroute group-address 224.3.2.1 sender-address 192.168.11.24 output-interface ethernet 1.2 CPE(config-ethernet1)# ip mroute group-address 224.3.2.1 sender-address 192.168.11.24 output-interface ethernet 0.3	Configura a interface com IP Multicast Routing Manual **Parâmetros:** *grp-addr*: endereço do grupo *src-addr*: endereço do emissor O exemplo configura o roteador com dois comandos para que todos os pacotes do grupo 224.3.2.1 com fonte 192.168.11.24 e recebidos na interface ethernet 0 sejam replicados para as interfaces ethernet 1.2 e 0.3, no caso, VLANs. Para remoção da configuração, utiliza-se o comando ***no***, e toda configuração de um grupo (IP fonte, IP multicast destino) é removida.

4.8.8.4. Protocol Independent Multicast (PIM)

Este protocolo é suportado em três modos. Dense, Sparse e Source Specific. Sendo que os últimos dois possuem configurações adicionais opcionais, mostradas mais adiante.

Para que ocorra o encaminhamento de pacotes multicast, é necessário que se ative o protocolo em mais de uma interface.

PIM Dense Mode

Ativar o roteamento multicast dinâmico com PIM Dense Mode é bastante simples: basta ativar a configuração na interface desejada, como mostrado na tabela abaixo.

Tabela 79: Configuração IP PIM Dense Mode

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface typenumber **Exemplo:** CPE (config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ip pim dense-mode	Configura a interface roteamento multicast dinâmico PIM Dense Mode.

PIM Sparse Mode

Ativar o roteamento multicast dinâmico com PIM Sparse Mode é bastante simples: basta entrar com os comandos mostrados na tabela abaixo.

Tabela 80: Configuração IP PIM Sparse Mode

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface typenumber **Exemplo:** CPE (config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ip pim sparse-mode	Configura a interface roteamento multicast dinâmico PIM Sparse Mode.

PIM Source Specific Mode

Ativar o roteamento multicast dinâmico com PIM Source Specific Mode é bastante simples: basta entrar com os comandos mostrados na tabela abaixo.

Tabela 81: Configuração IP PIM Source Specific Mode

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface typenumber **Exemplo:** CPE (config)# interface ethernet 1	Acessa o modo de configuração da interface.
4	CPE(config-interface)# ip pim ssm	Configura a interface roteamento multicast dinâmico PIM Source Specific Mode.

Configurações Adicionais

As configurações descritas nesta seção são usadas apenas pelo PIM modos Sparse e Source Specific. O modo PIM Dense não admite tais configurações, assim como o modo estático.

Candidate Bootstrap Router (Cand-BSR)

Por padrão, o roteador é um Candidate Bootstrap Router (RFC 5059). Para configurá-lo com uma prioridade específica, utilize os comandos da tabela abaixo.

Tabela 82: Configuração Candidate BSR

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# ip pimbsr-candidate { tunnel number | ethernet number}[priority value] **Exemplo:** CPE (config)# ip pim bsr-candidate ethernet 1 priority 128	Configura Candidate BSR. **Parâmetros:** number: número da interfaces value: valor da prioridade (0 a 255). Valores menores significam prioridades maiores. O exemplo configura o PIM para Candidate BSR na interface ethernet 1 com prioridade 128.

Rendezvous Point Address (RP-Address)

Por padrão, o PIM Sparse mode utiliza Auto-RP. Caso preferir, pode-se configurar um endereço de RP manualmente através dos comandos descritos na tabela abaixo.

Tabela 83: Configuração RP-Address

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip pim rp-address *address* **Exemplo:** *CPE(config)#* ip pim rp-address 192.168.11.245	Configura um RP com o endereço IP especificado. **Parâmetros:** *address:* endereço IP do Rendezvous Point. O exemplo configura um RP de endereço 192.168.11.245

PIMv2 RP Candidate (RP-Cand)

Por padrão, o roteador é um RP Candidate. Entretanto, é possível configurá-lo com parâmetros mais específicos, como prioridade e intervalo entre cada anúncio.

Tabela 84: Configuração RP-Candidate

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip pim rp-candidate { tunnel *number* | ethernet *number}*[interval *inverval*] [priority *priority*] **Exemplo:** *CPE(config)#* ip pim rp-candidate ethernet 1 interval 50	Configura RP Candidate. **Parâmetros:** *number:* número da interface *interval:*valor do intervalo em segundos entre cada anúncio RP-Candidate. *priority:*valor da prioridade (0 a 255). Valores menores significam prioridades maiores. O exemplo configura RP-Candidate na interface ethernet 0 com intervalo de anúncios de 50 segundos.

Visualização de Estatísticas

Com o comando show ip multicast é mostrada a configuração multicast de cada interface. Logo abaixo são mostrados todos os grupos multicast ativos, com contagem de pacotes e bytes encaminhados, além do modo de roteamento que cada grupo está operado.

Exemplo:

CPE>**show ip multicast**

IPv4 Multicast Summary

Interface:	Multicast Routing Mode:
ethernet 0.20	Static
ethernet 0	No multicast routing
ethernet 1	No multicast routing

Multicast Group:	Source:	Packets:	Bytes:	Routing:
224.3.2.1	192.168.11.35	132	78520	Static

4.8.9. Multi Protocol Label Switching

(recurso habilitado por licença)

MPLS é uma tecnologia de encaminhamento de pacotes que usa labels para tomar decisões de encaminhamento. A análise do cabeçalho da camada de rede é feita apenas uma vez (quando o pacote entra na rede MPLS). Depois disso os roteadores da rede MPLS encaminham os pacotes baseando-se apenas nos seus labels, que se situam entre a camada de enlace e a camada de rede de cada pacote. É por esse motivo que o protocolo MPLS é definido muitas vezes como pertencente à camada 2.5 do modelo OSI. Embora tenha um princípio de funcionamento muito simples, a utilização do protocolo MPLS permite a implementação de soluções de rede avançadas e com alta escalabilidade e baixos custos operacionais. As principais soluções MPLS utilizadas hoje são: MPLS L3VPN, MPLS L2VPN, VPLS e Engenharia de Tráfego.

4.8.9.1. Configuração

Na tabela abaixo são apresentados os procedimentos para habilitar o encaminhamento de pacotes MPLS e o protocolo LDP em uma interface:

Tabela 85: Configurando o encaminhamento de pacotes MPLS e o protocolo LDP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# mpls ip	Habilita o encaminhamento de pacotes MPLS e o LDP globalmente. Esse comando está habilitado por padrão e só precisa ser utilizado caso o comando no mpls ip tenha sido inserido anteriormente.
4	CPE (config)# interface type number	Acessa o modo de configuração da interface. OBS: apenas interfaces Ethernet e interfaces VLAN suportam MPLS.
5	CPE (config-interface)# mpls ip	Habilita o encaminhamento de pacotes MPLS e o LDP na interface. O encaminhamento de pacotes MPLS também precisa estar habilitado globalmente para que esse comando tenha efeito.

A tabela a seguir mostra a configuração de labels MPLS estáticos:

Tabela 86: Configurando LSPs estáticos

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# mpls static binding ipv4 netw-addr mask [input | output nexthop] label	Configura um label de entrada ou saída estático para um determinado prefixo IPv4. Labels de entrada estáticos têm precedência sobre labels de entrada alocados pelo LDP. Labels de saída alocados pelo LDP têm precedência sobre labels de saída configurados estaticamente. OBS: Não é possível configurar labels estáticos para prefixos locais.

A tabela abaixo mostra configurações adicionais para o LDP:

Tabela 87: Configurações adicionais para o LDP

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# mpls ldp discovery {hello {holdtime | interval} segundos | targeted-hello {holdtime | interval} segundos}	Configura o intervalo entre as transmissões de pacotes LDP Hello ou o tempo máximo que o roteador deve esperar sem receber nenhum pacote LDP Hello antes de fechar uma adjacência. Os valores padrão são: 15 segundos para o tempo máximo de espera de *link hellos* e 45 segundos para o tempo máximo de espera de *targeted hellos*. O intervalo de transmissão é de 5 segundos para ambos os casos.
	CPE (config)# mpls ldp discovery accept	Configura o roteador para aceitar requisições de criação de adjacências do tipo *targeted* de vizinhos que não estejam explicitamente configurados. Este comando não está habilitado por padrão.
	CPE (config)# mpls ldp explicit-null	Configura o roteador para anunciar o label *explicit-null* em ocasiões onde ele normalmente anunciaria o label *implicit-null*.
	CPE (config)# mpls ldp holdtime segundos	Configura o tempo máximo que o roteador deve esperar sem receber nenhuma mensagem LDP de um vizinho antes de fechar a respectiva sessão. O tempo máximo padrão é de 180 segundos.
	CPE (config)# mpls ldp neighbor password pswd-string	Configura autenticação MD5 para um determinado vizinho LDP.
	CPE (config)# mpls ldp neighbor targeted	Configura uma adjacência do tipo targeted com o vizinho especificado.

Comandos relacionados

CPE# show mpls forwarding-table	Exibe todos os mapeamentos MPLS instalados.
CPE# show mpls ip binding	Exibe todas as associações IP->MPLS instaladas.
CPE# show mpls ldp bindings [netw-addr/mask] [local-label label] [remote-label label] [neighbor address] [local]	Exibe todos os mapeamentos enviados e recebidos pelo LDP, mesmo os que não estão sendo utilizados.
CPE# show mpls ldp discovery	Exibe as adjacências LDP ativas.
CPE# show mpls ldp neighbor	Exibe os vizinhos LDP ativos.
CPE# show mpls static binding	Exibe os labels MPLS configurados estaticamente.

4.8.10. VRF-Lite

VRF (*Virtual Routing and Forwarding*) é uma tecnologia que permite que múltiplas instâncias da pilha TCP/IP coexistam ao mesmo tempo em um único roteador. Cada interface deve sempre estar associada a apenas uma VRF e interfaces de VRFs diferentes podem ter um mesmo endereço IP sem que haja um conflito. Por padrão todas as VRFs estão totalmente isoladas entre si, porém é possível configurar rotas estáticas ou o protocolo BGP para permitir o roteamento entre VRF diferentes. O conceito de VRFs foi introduzido pela solução MPLS VPN como forma de implementar a distribuição controlada de rotas de VPNs diferentes sem que haja a necessidade de usar roteadores adicionais. Apesar disso, o conceito de VRFs também pode ser útil mesmo fora do contexto de MPLS VPNs e nesse caso o termo VRF-Lite normalmente é utilizado.

4.8.10.1. Configuração

Na tabela abaixo são apresentados os procedimentos para criar uma VRF e associar uma interface a ela:

Tabela 88: Configurando uma VRF

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# vrf definition name	Configura uma VRF com o nome name e entra no modo de configuração da VRF.
4	CPE (config-vrf)# exit	Retorna para o modo de configuração.
5	CPE (config)# interface type number	Acessa o modo de configuração da interface.
6	CPE (config-interface)# vrf forwarding name	Associa a interface à VRF name. Ao mover uma interface de uma VRF para outra todos os seus endereços IP e IPv6 são perdidos e precisam ser configurados novamente caso necessário. Por padrão todas as interfaces pertencem à VRF global. Para que seja possível remover uma VRF nenhuma interface pode estar associada a ela.

Conforme pode ser visto ao longo deste manual, diversos comandos foram estendidos de forma a adicionar suporte a VRFs. O comando **ip route**, por exemplo, possui parâmetros que permitem criar rotas estáticas dentro de uma VRF ou até mesmo rotas estáticas entre VRFs diferentes (*Inter-VRF*). Outro exemplo é o comando **router ospf**, que possui um parâmetro adicional que permite especificar em qual VRF o processo OSPF será configurado.

Comandos relacionados

CPE# show vrf	Exibe as VRF configuradas e as interfaces associadas.

4.8.11. MPLS VPN

(recurso habilitado por licença)

A solução MPLS/BGP VPN (RFC4364) consiste de um conjunto de métodos utilizados por um provedor de serviços para oferecer VPNs (*Virtual Private Networks*) IP para os seus clientes. O protocolo MPLS é utilizado para realizar o transporte dos pacotes no *backbone* do provedor de serviços e o BGP é utilizado para distribuir as rotas das VPNs nesse *backbone*.

Essa solução usa o modelo de VPNs *peer-to-peer*, onde os roteadores do provedor de serviços, além de transportar o tráfego de seus clientes, também participam de seu roteamento. Nesse modelo deve haver ligações na camada de rede apenas entre os roteadores de borda do provedor de serviços (*Provider Edges*, PEs) e os roteadores de borda do cliente (*Consumer Edges*, CEs), e não uma série de conexões ponto a ponto entre os roteadores do cliente, como nas VPNs que usam o modelo *overlay*. Obtém-se a separação do tráfego das VPNs usando o conceito de VRF (*Virtual Routing Forwarding*) e o fato de os pacotes serem comutados no *backbone* do provedor de serviços utilizando o protocolo MPLS, e não roteados de acordo com os seus cabeçalhos IP. As VRFs são roteadores virtuais que utilizam tabelas de roteamento locais e separadas da tabela de roteamento global, que garantem o isolamento das informações de roteamento de diferentes clientes.

4.8.11.1. Configuração

A configuração de uma MPLS VPN se dá em várias etapas. Primeiro é preciso configurar uma ou mais VRFs e, para cada VRF, especificar um *RD (Rroute Distinguisher)* e um ou mais RTs (*Route-Targets)* de importação e de exportação. Depois é necessário configurar um protocolo de roteamento interno e habilitar o LDP nas interfaces usadas para transportar o tráfego das VPNs. Não existem restrições quanto aos protocolos de roteamento interno que podem ser utilizados. Por fim, é necessário configurar o MP-BGP para distribuir as rotas das VPNs.

4.8.11.1.1. VRF

Na tabela abaixo são apresentados os procedimentos para configurar uma VRF com os parâmetros necessários para a sua utilização em uma MPLS VPN.

Tabela 89: Configurando uma VRF para MPLS VPN.

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# vrf definition name	Configura uma VRF e entra no modo de configuração da VRF.
4	CPE (config-vrf)# rd route-distinguisher	Configura um RD.
5	CPE (config-vrf)# address-family ipv4	Entra no modo de configuração da address-family IPv4 da VRF.
6	CPE (config-vrf)# route-target {import | export | both} route-target-ext-community	Configura um RT de importação, exportação ou ambos para a VRF. Múltiplos RTs podem ser definidos para uma mesma VRFs.

4.8.11.1.2. MP-BGP

Na tabela abaixo são apresentados os procedimentos para configurar o BGP para redistribuir as rotas das VRFs e anunciá-las para um neighbor usando para isso a adress-family VPNv4:

Tabela 90: Configurando o BGP para uma MPLS VPN

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# router bgp as-number	Acessa o modo de configuração do BGP.
4	CPE(config-bgp)# neighbor neighbor-addr remote-as as-number	Configura um neighbor BGP.
5	CPE(config-bgp)# address-family ipv4 vrf name	Entra no modo de configuração da address-family IPv4 da VRF name.
6	CPE(config-bgp-af)# redistribute {bgp | connected | kernel | ospf | static}	Configura a redistribuição de rotas da VRF para a tabela VPNv4 do BGP.
7	CPE(config-bgp-af)# exit	Sai do modo de configuração da address-family IPv4 da VRF.
8	CPE(config-bgp)# address-family vpnv4 unicast	Entra no modo de configuração da address-family VPNv4 unicast
9	CPE(config-bgp-af)# neighbor neighbor-addr activate	Ativa a distribuição de rotas VPNv4 com esse neighbor.

Comandos relacionados

CPE# show bgp vpnv4 unicast all [labels]	Exibe a tabela VPNv4 do BGP.
CPE# show bgp vpnv4 unicast summary	Exibe os neighbors configurados para roteamento VPNv4.
CPE# show ip route vrf name	Exibe a tabela de roteamento IPv4 de uma VRF.

4.9. Authentication, Authorization e Accounting – AAA

O AAA (Authentication, Authorization e Accounting) oferece métodos para autenticar usuários para o acesso a dispositivos de rede, controlar o nível de acesso destes usuários para os recursos disponíveis e armazenar informações relacionadas aos comandos executados em cada sessão.

Na etapa de autenticação, a identidade do usuário é verificada após o fornecimento do login e senha. Na autorização, esta pode ser realizada de duas formas: em um momento único, logo após a autenticação e neste caso, permitindo o acesso do usuário autorizado a todos os comandos disponíveis ou ainda, de forma individual para cada comando a ser executado. Já a última etapa, o accounting consiste no envio de informações relacionadas aos comandos executados, incluindo informações de tempo, usuário, entre outras.

O CPE pode autenticar e controlar o acesso de usuários aos comandos localmente com 15 diferentes níveis de usuários, trazendo flexibilidade para o processo de configuração das permissões de cada usuário. Além disso, o equipamento implementa o AAA via RADIUS e TACACS+ com possibilidade de configurar backup para a base de dados local em caso de indisponibilidade do(s) servidor(es).

A seguir são apresentadas as configurações de usuários no CPE e as funcionalidades do AAA presentes no equipamento, bem como os procedimentos para a configuração das mesmas.

4.9.1. Adição de usuários na base de dados do CPE

O CPE permite a configuração de 15 níveis de usuários (de 1 até 15), sendo o 15 o usuário mais privilegiado. Desta forma é possível ter um controle flexível dos direitos de cada nível de usuário, comando a comando.

A seguir são apresentados os comandos para adição de usuários:

Tabela 91: Configuração de usuários

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] username user privilege priv-level {nopassword | password pass} **Exemplo:** CPE (config)# username adminprivilege 15password secret123	Adiciona ou remove um usuário com o privilégio indicado após privilege (de 1 até 15, sendo 1 o usuário menos privilegiado). No exemplo é configurado um usuário com privilégio máximo.

A seguir são descritas as etapas para configuração do enable secret, que permite ao usuário acessar o modo privilegiado:

Tabela 92: Configuração do enable secret

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# enable secret level priv-level secret-word **Exemplo:** CPE (config)# enable secret level 7 secret777	Configura o enable secret para um nível de privilégio específico. Para remover um enable secret: **no enable secret level priv-level** No exemplo é definido o enable secret para o nível de privilégio 7.

Comandos relacionados

CPE (config)# aaa new-model	Habilita as funcionalidades de AAA.
CPE (config)# aaa authentication {enable | login | ppp} {default | service {console | ftp | ssh | telnet}} {local | group {radius[local] | tacacs+[local]} | none} **Exemplo:** CPE (config)# aaa authentication login default local	Configura o modo de autenticação para acesso ao equipamento ou protocolo PPP. É possível definir modo de autenticação para todos os serviços ou para um serviço específico com a palavra chave **service.** A autenticação pode ser realizada localmente ou com grupos de servidores Radius ou Tacacs+. Para desabilitar a autenticação utiliza-se: **aaa authentication {enable | login | ppp} default none**. No exemplo, configura-se a autenticação local para o login.

4.9.2. Radius e TACACS+

O RADIUS (Remote Authentication Dial In User Service)(RFC 2865) (RFC 2866) e o TACACS+ (Terminal Access Controller Access-Control System) (Tacacs+ Internet Draft) são protocolos destinados a autenticação, autorização e contabilização de comandos em redes de computadores. O RADIUS utiliza transporte UDP, enquanto que o TACACS+ executa sobre TCP. Ambos possuem arquitetura cliente-servidor, sendo que o CPE atua como cliente.

As transações entre cliente e servidor são autenticadas através do uso de uma chave compartilhada. Com uso de RADIUS, somente a senha é criptografada para ser enviada pela rede, enquanto que com TACACS+ é possível criptografar toda a mensagem. Além disso, o TACACS+ separa bem os processos de autenticação, autorização e contabilização, diferentemente do que acontece com o RADIUS, que trata autorização e autenticação em conjunto e separa o accounting.

4.9.2.1. Configurações do RADIUS

Abaixo são mostrados os procedimentos para configurar o AAA via Radius:

Tabela 93: Configurações do AAA via Radius

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# aaa new-model	Habilita o AAA.
4	CPE (config)# [no] radius-server host ip-addr[key string][timeout seconds] [acc-port port] [port port] **Exemplo:** CPE (config)# radius-server host 192.168.1.12:9876 key secret123 timeout 2	Adiciona ou remove um servidor RADIUS e opcionalmente uma porta UDP. **Parâmetros:** **port:** A porta padrão é a 1812 para autenticação e a 1813 para o accounting. Se uma porta especifica é configurada para a autenticação, a porta subsequente é utilizada para o accounting. **key:** Chave usada para criptografar a senha. Deve ser a mesma configurada no servidor Radius. **timeout:** Tempo em segundos que o equipamento espera por uma resposta do servidor antes de retransmitir a requisição. No exemplo, as requisições de autenticação são enviadas para a porta 9876 do servidor configurado e o cliente aguardará dois segundos antes de retransmitir as requisições. O accounting será enviado para a porta 9877.
5	CPE (config)# aaa authentication login default group radius local	Após configurar o servidor Radius, é definido como método de autenticação principal o Radius e em caso de falha do(s) servidor(es), deve ser feita a autenticação com consulta a base de dados do equipamento. Nesse caso, o mesmo usuário e senha existentes no servidor devem ser configurados localmente também, através do comando **aaa username**. Para remover a configuração: **aaa authentication login default none**
6	CPE (config)# aaa authorization exec default group radius local	Configura a autorização do exec (terminal) para ser feita via Radius. As informações referentes a autorização são retornadas na resposta da autenticação. Em caso de indisponibilidade do servidor, a autorização é feita localmente (neste caso, todo o usuário autenticado é autorizado). Para remover a configuração: **aaa authorization exec default none**
7	CPE (config)# aaa accounting exec default start-stop group radius	Configura o envio do accounting no momento do acesso ao terminal (logo após a autenticação) e no final da sessão. Para remover a configuração: **aaa accounting exec default none**

4.9.2.2. Configurações do TACACS+

Tabela 94: Configurações do AAA via Tacacs+

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# aaa new-model	Habilita o AAA.
4	CPE (config)# [no] tacacs-server host ip-addr [key string][timeout seconds][port port] **Exemplo:** CPE (config)# tacacs-server host 192.168.1.12 port 9999 key secret123 timeout 2	Adiciona ou remove um servidor Tacacs+ e uma opcionalmente uma porta TCP. **Parâmetros:** **port:** A porta padrão é a 49. Também é possível configurar outra porta, de 1 até 65534. **key:** Chave usada para criptografar as mensagens. Deve ser a mesma configurada no servidor Tacacs+. **timeout:** Tempo em segundos que o equipamento espera por uma resposta do servidor antes de retransmitir a requisição. No exemplo tem-se o servidor Tacacs+ no endereço IP 192.168.1.12 escutando a porta TCP 9999. O segredo compartilhado entre o servidor e seus clientes é “secret123” e o timeout para uma requisição enviada é 2 segundos.
5	Autenticação 1) Login CPE (config)# aaa authentication login {default | service {console | ftp | ssh | telnet}} {[group tacacs+] [group radius] [local] [none]} 2) Enable e PPP CPE (config)# aaa authentication {enable | ppp} default [group tacacs+] [group radius] [local] [none]	Após configurar o servidor Tacacs+, é definido como método de autenticação principal o Tacacs+. Opcionalmente, pode ser configurada a autenticação via Radius (que será realizada em caso de falha do(s) servidor(es) Tacacs+). Neste caso, é indispensável configurar o mesmo usuário e senha em todos os servidores. No exemplo 1, se os servidores Tacacs e Radius estiverem indisponíveis não será possível ter acesso ao equipamento. Também pode ser configurado o backup para a base de dados do equipamento. Nesse caso, o mesmo usuário e senha existentes no(s) servidor(es) devem ser configurados localmente também, através do comando **aaa username**. No exemplo 3, a primeira tentativa de autenticação é via Tacacs+ e em caso de falha do(s) servidores, via Radius. Se em ambos os casos não for recebida nenhuma resposta, a autenticação é feita

	3) Para desabilitar a autenticação do login CPE (config)# aaa authentication login {default | service {console | ftp | ssh | telnet}} none 4) Para desabilitar a autenticação do enable e PPP CPE (config)# aaa authentication {enable | ppp} default none **Exemplos:** 1) Tacacs+ e Radius CPE (config)# aaa authentication login default group tacacs group radius 2) Tacacs+ e local CPE (config)# aaa authentication login default group tacacs local 3) Tacacs+, Radius e local CPE (config)# aaa authentication login default group tacacs group radius local	localmente. **Importante: Para evitar a perda de acesso ao equipamento, é recomendável que o usuário e senha a serem utilizados sejam previamente configurados nos servidores e/ou localmente.** **Além disso, se após configurar a autenticação for desejado proceder com as configurações de autorização, é recomendável encerrar a sessão executando o comando exit duas vezese então, entrar com o usuário e senha recém configurados. Observadas estas recomendações, pode-se passar para as próximas etapas.**
6	Autorização: CPE (config)# aaa authorization exec default group tacacs+ [local]	Configura a autorização do exec (terminal) para ser feita via Tacacs+. O pedido de autorização é enviado logo após a conclusão da autenticação. Em caso de indisponibilidade do servidor, a autorização pode (opcionalmente) ser feita localmente (neste caso, todo o usuário autenticado é autorizado). Para desabilitar a autorização do exec: **aaa authorization exec default none**

7	CPE (config)# aaa authorization commands {privileged | user} default { group tacacs+ [local] | none}	Configura a autorização individual via Tacacs+ para cada comando, para comandos executados no modo exec (raiz), nos modos privilegiado (enable) ou usuário. O backup para a base de dados do equipamento é opcional e neste caso, um usuário nível 15 poderá executar todos os comandos enquanto que os demais usuários terão direito a executar os comandos definidos para o seu nível. Os níveis de usuário default existentes no equipamento são 1 e 15 (superusuário). Para configurar outros níveis, consulte a tabela "Configuração de usuários". Para configurar um nível de privilégio um comando específico, consulte a tabela "Configuração de níveis de privilégios para os comandos". Para desabilitar a autorização de comandos: **aaa authorization commands {privileged | user} default none**
8	CPE (config)# aaa authorization config_commands default { group tacacs+ [local] | none}	Configura a autorização de comandos globais de configuração. Com esta opção ativada, executando-se o comando **configure terminal**, todos os comandos subsequentes serão autorizados individualmente via Tacacs+ ou em caso de falha do(s) servidor(es), localmente. Para desabilitar a autorização dos comandos globais: **aaa authorization config_commands {privileged | user} default none**
9	CPE (config)# aaa accounting exec default {start-stop group {radius | tacacs+} | none}	Configura o accounting do exec via Radius ou Tacacs+, que será enviado no início e no final de cada sessão. Para desabilitar o accounting do exec: **aaa accounting exec default none**
10	CPE (config)# aaa accounting commands {privileged | user} default { start-stop group tacacs+ | none }	Configura o accounting dos comandos para os modos privilegiado (enable) ou usuário. O accounting será enviado a cada execução de comando. Para desabilitar o accounting dos comandos: **aaa accounting commands {privileged | user} default none**

Tabela 95: Configuração de níveis de privilégios para os comandos

Passo	Comando	Objetivo
1	CPE> enable	Acessa o modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] privilege mode{all level | level}priv-levelcommand **Exemplo:** CPE (config)# privilege exec level 7 configure terminal CPE (config)# privilege configure level 7 interface CPE (config)# privilege configure level 7 snmp-server	Configura/remove o nível de privilégio necessário para a execução de um comando. No exemplo, para os usuários de nível 7, no modo exec (que é acessado após a execução do comando **enable)** é permitido somente o comando **configure terminal**. Após executar este comando é acessado o modo de **configuração global**, onde são permitidos somente os comandos **snmp-server** e **interface**. Além dos comandos mencionados, **exit** e **end** também estarão disponíveis. Para os casos em que a autorização é feita via servidor Tacacs+, o pedido de autorização só é enviado quando o comando que o usuário tenta executar é compatível com o seu privilégio.

4.10. Quality of Service (QoS)

QoS é a habilidade de fornecer diferentes prioridades ou garantias para usuários, aplicações, fluxos ou dados diferentes. Prioridades e garantias são importantes quando a capacidade da rede é insuficiente, especialmente para aplicações que requerem largura de banda ou parâmetros de jitter e atraso específicos para o correto funcionamento.

Redes configuradas com QoS são capazes de prover um serviço melhor e mais previsível ao implementarem os seguintes serviços:

- Garantia de Largura de Banda
- Configuração de Características de Perda e Descarte de Pacotes
- Controle e Prevenção de Congestionamento
- Conformação e Policiamento de Tráfego
- Configuração de Prioridades
- É importante que o leitor tenha conhecimentos básicos de comutação de pacotes em redes, Precedência IP e DSCP para uma melhor compreensão desta seção.

4.10.1. Visão Geral dos Mecanismos Suportados

São suportados mecanismos de controle e prevenção de congestionamento, policiamento e conformação de tráfego, além de Traffic Policies. Abaixo, serão dadas noções sobre cada grupo de mecanismos e também sobre os mecanismos em si.

Mecanismos de Controle de Congestionamento: estes mecanismos operam para controlar o congestionamento uma vez que este ocorre. De modo geral, pacotes são colocados em uma fila e encaminhados segundo alguma regra específica, dependendo do mecanismo instalado. Cada mecanismo é específico para resolver algum tipo de problema na rede e suas propriedades, na maioria das vezes, são completamente diferentes. Os mecanismos de controle de congestionamento suportados estão listados abaixo.

- PFIFO FAST. FIFO é um mecanismo não preemptivo que encaminha pacotes por ordem de chegada, o primeiro a chegar é o primeiro a sair. PFIFO-FAST utiliza três filas FIFO de prioridades diferentes. O tráfego é enfileirado em cada fila de acordo com o Type of Service (ToS). No caso de congestionamento, filas de menor prioridade só são servidas quando as de maior prioridade estão vazias.

- Stochastic fair queueing (SFQ). SFQ é um mecanismo que divide todo tráfego em fluxos, classificando-o de acordo com endereços IP de destino e origem, portas e protocolos. No caso de congestionamento, cada fluxo recebe uma fatia justa da banda disponível.

- Weighted fair queueing (WFQ). WFQ é um mecanismo que classifica o tráfego em oito classes distintas, de acordo com precedência IP. Classes de precedência são servidas com mais frequência (Weighted). Ressalta-se que todas as classes são sempre servidas, não importando o grau de congestionamento da rede. Além disso, os fluxos de cada classe são tratados de maneira justa (Fair Queueing).

- Custom queueing (CQ). CQ é um mecanismo configurável. São 16 classes disponíveis, servidas por um mecanismo do tipo Round-Robin. Toda vez que uma classe é servida, um número máximo de bytes é encaminhado. É possível configurar este número em cada classe, assim como o tamanho máximo de cada uma.

- Priority queueing (PQ). PQ também é um mecanismo configurável. São 4 classes de prioridades distintas (High, Medium, Normal e Low). Durante congestionamento, pacotes pertencentes à uma classe de prioridade mais alta são enviados antes de todos os pacotes de classes de prioridade mais baixa. Ou seja, prioridades mais altas passam sempre na frente e, em casos extremos, prioridades mais baixam podem nunca ser servidas.

- IP Voip Priority. O IP Voice Priority foi criado especialmente para lidar com tráfego de voz. Este tráfego é sempre passado à frente enquanto todo resto é servido de acordo com precedência IP. (Apenas nos modelos com VoIP)

Mecanismos de Prevenção de Congestionamento: diferentes dos mecanismos de controle de congestionamento, os mecanismos de prevenção não agem apenas quando o congestionamento de fato ocorre. Estes mecanismos monitoram a carga da rede e agem para prevenir que a rede venha a congestionar, melhorando significativamente sua utilização. Os mecanismos de prevenção de congestionamento suportados estão listados abaixo.

- Random Early Detect (RED). Os mecanismos de controle de congestionamento apenas descartam pacotes quando seus buffers estão cheios, causando problemas como TCP global synchronization: a rede oscila entre os estados de congestionamento total e subutilização. Para evitar isso e aproveitar melhor a infraestrutura disponível, o mecanismo RED começa lentamente a descartar pacotes (ou marcar com Explicit Congestion Notification – ECN) conforme seu buffer vai enchendo, aumentando a probabilidade de descarte de acordo com o tamanho da fila. Este comportamento faz com que conexões TCP diminuam suas taxas de envio antes do congestionamento ocorrer, evitando-o.

- Weighted Random Early Detect (WRED). O WRED nada mais é do que uma RED que leva em conta precedência IP ou DSCP (configurável) para o descarte antecipado de pacotes. Por exemplo: conforme a fila vai enchendo, pacotes de IP Precedence ou DSCP menores tem maior probabilidade de serem descartados do que pacotes de IP Precedence ou DSCP maiores.

- Stochastic Fair Blue (SFB). O SFB faz parte de uma nova geração de mecanismos de prevenção de congestionamento. Ele é mais inteligente que os mecanismos RED, ajustando seus parâmetros automaticamente de acordo com as características do tráfego e lidando de forma muito melhor com tráfego que não responde a perda de pacotes ou notificação de congestionamento. Inicialmente, o tráfego é classificado em fluxos, assim como na SFQ. A SFB é justa na alocação de espaço no buffer para cada fila, ela age para garantir que cada fluxo ganhe uma fatia justa do buffer. Fluxos que estão ocupando muito espaço no buffer têm mais pacotes descartados ou marcados com ECN. Caso este fluxo não responda a estas ações, diminuindo sua taxa de envio, a SFB coloca o fluxo na “caixa de castigo”, junto com outros fluxos mal comportados. Os fluxos desta caixa têm suas bandas limitadas por um certo tempo. Neste sentido, a SFB lida muito bem com fluxos mal comportados, ao contrário da RED, que aplica a mesma probabilidade de descarte para os fluxos que responderam bem e para os que não responderam às medidas tomadas.

Mecanismos de Policiamento e Conformação de Tráfego: os mecanismos de policiamento e conformação identificam violações de parâmetros (geralmente taxa de envio e recebimento) e tomam ações diferentes para lidar com estas violações. O policiamento tem como característica simplesmente descartar qualquer pacote que viole os parâmetros configurados, enquanto a conformação geralmente armazena este pacote e apenas o encaminha quando é possível fazê-lo sem violar os parâmetros configurados.

- Rate Limit. É possível policiar as taxas de entrada e saída em uma interface. Por exemplo, limitar um determinado DSCP a uma certa taxa entrando em alguma interface. Ou ainda, restringir a banda de saída de um determinado protocolo e faixa de portas em uma outra interface qualquer.

- Traffic Shape. Conformação de tráfego, feita apenas no sentido de saída da interface. Tem como característica um enorme buffer, capaz de armazenar muitos pacotes. Em períodos que a taxa de entrada é maior do que a de saída, ocorre a acumulação de pacotes. Quando a taxa de entrada é menor do que a de saída, os pacotes armazenados começam a ser enviados, e o número de pacotes armazenados decai. O resultado disso é uma taxa constante na saída, independente da taxa de entrada. Evidentemente, existem limites físicos de memória para isso.

- Traffic Policy. Esta ferramenta possibilita a criação de soluções QoS customizadas. Por exemplo, deseja-se usar WFQ para um determinado tipo de tráfego e WRED para outro. Com ela, ainda é possível realizar marcação de pacotes (sinalização) e controle de taxas. Serão discutidos em uma seção separada mais adiante.

  Dada esta visão geral de QoS, é importante ressaltar que nem todos mecanismos podem ser utilizados simultaneamente. Na tabela abaixo são mostradas as combinações possíveis. Em resumo, todas funcionalidades podem ser combinadas, desde que se escolha apenas uma entre Controle de Congestionamento, Traffic Policy e Prevenção de Congestionamento. Sendo que, de fato, Traffic Policy pode combinar Controle de Congestionamento e Prevenção de Congestionamento. Na prática, qualquer configuração pode ser feita, desde que se utilize as ferramentas corretas.

Tabela 96: Combinações Possíveis de Mecanismos QoS

Mecanismo	Controle de Congestionamento	Traffic Policy (CBWFQ)	Prevenção de Congestionamento	Conformação	Policiamento
Controle de Congestionamento	-	NÃO	NÃO	SIM	SIM
Traffic Policy (CBWFQ)	NÃO	-	NÃO	SIM	SIM
Prevenção de Congestionamento	NÃO	NÃO	-	SIM	SIM
Conformação	SIM	SIM	SIM	-	SIM
Policiamento	SIM	SIM	SIM	SIM	-

4.10.2. Controle de Congestionamento

PFIFO FAST

PFIFO FAST é o mecanismo padrão configurado nas interfaces. Se não houver nenhuma outra configuração de controle, conformação de tráfego ou prevenção de congestionamento na interface, este será o mecanismo ativo.

Stochastic Fair Queueing (SFQ)

SFQ é um mecanismo que distribui igualmente largura de banda para os diferentes fluxos. Ela garante que nenhum fluxo obtenha toda banda enquanto outros fiquem sem serviço. Sua configuração é simples e dispensa parâmetros. Abaixo estão listados os comandos para configurar Stochastic Fair Queueing.

Tabela 97: Configuração de QoS SFQ

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)# sto-fair-queue **Exemplo:** CPE(config-ethernet0)# sto-fair-queue	Configura SFQ para interface. O exemplo habilita SFQ na interface ethernet 0.

Weighted Fair Queueing (WFQ)

O WFQ é diferente do SFQ. A WFQ trabalha com classes de diferentes pesos, enquanto a SFQ se baseia na distribuição igualitária entre os fluxos. Classes com precedência IP maior têm maior banda alocada. Sua configuração também é simples. Abaixo estão listados os comandos para configurar Weighted Fair Queueing.

Tabela 98: Configuração de QoS WFQ

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)# fair-queue **Exemplo:** CPE(config-ethernet0)# fair-queue	Configura WFQ para interface. O exemplo habilita WFQ na interface ethernet 0.

Custom Queueing (CQ)

CQ é um mecanismo bastante customizável. Até 16 filas podem ser configuradas. Elas são servidas por escalonador do tipo Round Robin, em que cada fila recebe um quantum, valor este que diz o número de bytes que uma fila pode enviar até o próximo escalonamento. Além das regras de classificação dos pacotes, é possível configurar o quantum e o tamanho máximo de cada fila. Abaixo estão listados os comandos para configurar Custom Queueing. A configuração é feita em dois passos, o primeiro é configurar uma queue-list, mostrado na tabela abaixo. Todos os comandos são obrigatórios, exceto quando especificados como opcionais.

Tabela 99: Configuração de QoS Custom Queueing – queue-list

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# queue-list list default queue **Exemplo:** CPE(config)# queue-list 5 default 11	(Opcional) Configura a fila padrão da queue-list. **Parâmetros:** list: número da queue-list queue: número da fila (1-16) **Atenção:** Caso não seja configurado, pacotes não classificados são descartados. O exemplo mostra uma configuração de queue-list que todos pacotes não classificados vão para a fila 11.
	CPE(config)# queue-list list interface interface number queue **Exemplo:** CPE(config)# queue-list 5 interface ethernet 1 9	(Opcional) Associa todos pacotes oriundos de uma interface à uma fila. **Parâmetros:** list: número da queue-list interface number: interface queue: número da fila (1-16) O exemplo mostra uma configuração de queue-list que todos os pacotes vindos da interface ethernet 1 são enfileirados na fila 9.
	CPE(config)# queue-list list queue queue { byte-cout quantum | limit packets} **Exemplo 1:** CPE(config)# queue-list 5 queue 4 byte-count 3000 **Exemplo 2:** CPE(config)# queue-list 5 queue 4 limit 80	(Opcional) Configura os tamanhos das filas de prioridade, por número de pacotes. **Parâmetros:** list: número da queue-list queue: número da fila (1-16) quantum: quantum da fila no algoritmo de round roubin (padrão 1500 bytes) packets: número máximo de pacotes na fila (padrão 20 pacotes) O exemplo 1 mostra a configuração de 3000 bytes de peso para a fila 4 para o algoritmo de RR da queue-list 5. O exemplo 2 mostra uma configuração de 80 pacotes como tamanho máximo da fila 4 da queue-list 5.

	CPE(config)#queue-list list protocol { aarp | arp | ipx | loop } queue **Exemplo:** CPE(config)# queue-list 5 protocol ipx 7	(Opcional) Configura todos pacotes de um determinado protocolo para uma fila específica. **Parâmetros:** list: número da queue-list queue: número da fila (1-16) O exemplo mostra uma configuração de queue-list que todos pacotes ipx são enfileirados na fila 7. Nota: Os protocolos ip e ipv6 possuem mais opções e são mostrados abaixo.
	CPE(config)#queue-list list protocol { ip | ipv6 } queue { list acess-list | rtp***** | sip***** } ***** apenas para equipamentos com VoIP **Exemplo:** CPE(config)# queue-list 5 protocol ip 2 list 101	(Opcional) Configura os pacotes ip ou ipv6, de uma acess-list, sip ou voz, para serem enfileirados em uma fila específica. **Parâmetros:** list: número da queue-list queue: número da fila (1-16) acess-list: número da acess list. O exemplo mostra uma configuração de queue-list que todos pacotes ip relacionados a access-list 101 são enfileirados na fila 2

O segundo passo é aplicar esta queue-list em uma interface. Os comandos são mostrados na tabela abaixo.

Tabela 100: Configuração de QoS Custom Queueing – custom-queue-list

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	Digistar-CPE(config)# interface type number **Exemplo:** CPE(config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)# custom-queue-list queue-list **Exemplo:** CPE(config-ethernet0)# custom-queue-list 5	Configura CQ para interface. **Parâmetros:** queue-list: número da queue-list que contém as configurações desejadas. O exemplo configura CQ na interface ethernet 0, de acordo com o queue-list 5.

Priority Queueing (PQ)

A configuração de PQ é feita em dois passos. O primeiro é configurar uma priority-list. É nesta configuração que são definidas as propriedades de QoS da PQ. A primeira tabela abaixo mostra a configuração de uma priority-list. Todos os comandos são obrigatórios, exceto quando especificados como opcionais.

Tabela 101: Configuração de QoS Priority Queueing – priority-list

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# priority-list list default { high | medium | normal | low } **Exemplo:** CPE(config)# priority-list 3 default low	(Opcional) Configura uma priority-list para ter como prioridade padrão high, medium, normal ou low. Caso não seja configurado, o valor padrão da prioridade padrão é normal. **Parâmetros:** list: número da priority-list interface number: interface O exemplo mostra uma configuração de priority list que todos pacotes não classificados têm prioridade low.
	CPE(config)#priority-list list interface interface number { high | medium | normal | low } **Exemplo:** CPE(config)# priority-list 3 interface ethernet 1 high	(Opcional) Configura todos pacotes oriundos de uma interface com uma prioridade. **Parâmetros:** list: número da priority-list O exemplo mostra uma configuração de priority list que todos os pacotes vindos da interface ethernet 1 são classificados como high.
	CPE(config)#priority-list list queue-limit high normal medium low **Exemplo:** CPE(config)# priority-list 3 queue-limit 80 60 40 20	(Opcional) Configura os tamanhos das filas de prioridade, por número de pacotes. **Parâmetros:** list: número da priority-list high: número pacotes antes de ocorrer tail-drop na fila de prioridade high. medium: número pacotes antes de ocorrer tail-drop na fila de prioridade medium. normal: número pacotes antes de ocorrer tail-drop na fila de prioridade normal. low: número pacotes antes de ocorrer tail-drop na fila de prioridade low. O exemplo mostra uma configuração de priority list que a fila high armazena até 80 pacotes, a medium 60 pacotes, a normal 40 e a low 20.

	CPE(config)#priority-list list protocol { aarp | arp | ipx | loop } { high | medium | normal | low } **Exemplo:** CPE(config)# priority-list 3 protocol ipx medium	(Opcional) Configura todos pacotes de um determinado protocolo com uma prioridade. **Parâmetros:** list: número da priority-list O exemplo mostra uma configuração de priority list que todos pacotes ipx são classificados como medium. Nota: os protocolos ip e ipv6 possuem mais opções e são mostrados abaixo.
	CPE(config)#priority-list number protocol { ip | ipv6 } { high | medium | normal | low } { list acess-list | sip***** | rtp***** } ***** apenas para equipamentos com VoIP **Exemplo:** CPE(config)# priority-list 3 protocol ip normal list 104	(Opcional) Configura os pacotes ip ou ipv6, de uma acess-list, tcp ou udp de determinadas portas com uma prioridade. **Parâmetros:** number: número da priority-list. acess-list: número da acess list. O exemplo mostra uma configuração de priority list que todos pacotes ip relacionados a access-list 104 são classificados como normal.

O segundo passo é aplicar a priority-list em uma interface, mostrado na tabela abaixo.

Tabela 102: Configuração de QoS Priority Queueing – priority-group

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE (config-interface)# priority-group Priority Group **Exemplo:** CPE(config-ethernet0)# priorty-group 3	Configura PQ para interface. **Parâmetros:** Priority Group: número da priority list que contém as configurações desejadas. O exemplo configura Priority Queueing na interface ethernet 0, de acordo com o priority list 3.

IP VOIP Priority (apenas modelos com VoIP)

IP VoIP Priority é uma ferramenta para priorizar tráfegos de voz. Este comando aplica prioridade estrita para os pacotes SIP, seguidos pelos pacotes de voz (RTP) e por último o tráfego geral. É necessário configurar o número da porta SIP. Opcionalmente, pode-se configurar para que os pacotes de voz TCP também sejam priorizados. Além disso, um de limite de banda de download e upload pode ser estabelecido na interface. Esta funcionalidade é mutuamente exclusiva com qualquer outra funcionalidade de QoS.

Importante: este comando está disponível apenas em modelos que tem VoIP.

Tabela 103: Configuração de QoS IP VOIP Priority

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE (config-interface)# ip voip priority port [tcp] [download upload] **Exemplo:** CPE(config-ethernet0)# ip voip priority 5060 2M 10M	Configura IP VOIP Priority para interface. **Parâmetros:** port: número da porta SIP tcp: habilita priorização de pacotes tcp também download: limita taxa de input na interface. upload: limita taxa de output na interface. O exemplo configura um IP VoIP Priority com porta SIP 5060 e limite de envio de 2Mbps e recepção de 10Mbps.

4.10.3. Prevenção de Congestionamento

Random Early Detect (RED)

Para a configuração de filas RED é aconselhável que se busque ajuda na literatura para a correta configuração deste tipo de fila. Abaixo estão listados os comandos para configurar Random Early Detect.

Tabela 104: Configuração de QoS RED

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE (config-interface)# custom-random-detect Minimum threshold Maximum threshold Queue limit Mark probability denominator Traffic Burst **Exemplo:** CPE(config-ethernet0)# custom-random-detect 20 50 99 200 25	Configura RED para interface. **Parâmetros:** Minimum threshold: número mínimo de pacotes na fila para que o descarte comece. Maximum threshold: número de pacotes na fila para que a taxa de descarte seja <Mark probability denominator> Queue limit: tamanho máximo da fila. Quando a fila estiver com este número de pacotes, todos os novos pacotes serão descartados. Mark probability denominator: um a cada quantos pacotes deve ser descartado. Para Mark probability denominator = 99, 1 a cada 99 pacotes será descartado. Traffic Burst: número de pacotes permitidos em um burst. **Atenção:** estes parâmetros devem ser cuidadosamente calculados para cada aplicação. Uma RED com parâmetros incorretos pode causar efeitos indesejáveis. O exemplo configura na interface ethernet 0 uma RED que começa a descartar quando a fila atige 20 pacotes, descarta 1 a cada 99 quando a fila atinge 50 pacotes, descarta todos pacotes quando a fila atinge 200 pacotes e permite bursts de até 25 pacotes.

Weighted Random Early Detect (WRED)

A WRED nada mais é do que uma RED que suporta parâmetros diferentes para cada classe. Embora seja mais complexa, a WRED é mais simples de ser configurada. Abaixo estão listados os comandos para configurar Weighted Random Early Detect.

Tabela 105: Configuração de QoS WRED

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)#random-detect [dscp-based | prec-based] **Exemplo:** CPE(config-ethernet0)#random-detect	Configura WRED para interface. A WRED pode operar em dois modos: **Parâmetros:** c-based (default): curvas de descarte distintas para IP Precedence distintos p-based: curvas de descarte distintas para DSCPs distintos. O exemplo habilita WRED baseada em IP Precedence na interface ethernet 0.

Stochastic Fair Blue (SFB)

Embora seja uma fila bastante sofisticada, sua configuração é extremamente simples, pois os parâmetros são automaticamente calculados de forma dinâmica. Abaixo estão listados os comandos para configurar Stochastic Fair Blue.

Tabela 106: Configuração de QoS SFB

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	Digistar-CPE(config-interface)#sto-fair-blue **Exemplo:** CPE(config-ethernet0)#sto-fair-blue	Configura SFB para interface. O exemplo habilita SFB na interface ethernet 0.

4.10.4. Policiamento e Conformação de Tráfego

Rate-Limit Simples

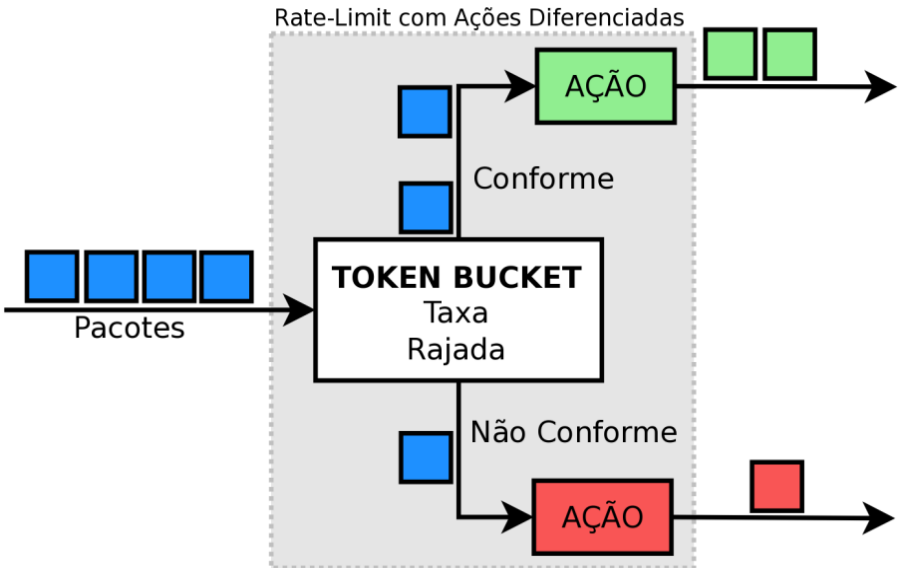
Rate-Limit é uma forma de policiamento de tráfego. É criada uma limitação de taxa de envio ou recebimento de pacotes. Os pacotes de excederem esta taxa são descartados. Abaixo estão listados os comandos para configurar Rate-Limit.

Tabela 107: Configuração de Rate Limit

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)#rate-limit { input | output } rate **Exemplo:** CPE(config-ethernet0)#rate-limit output 5M	Configura limitação de taxa para interface. Pode ser configurado no sentido de entrada (input) ou saída (output). **Parâmetros:** rate: taxa máxima permitida O exemplo limita a taxa de saída da interface ethernet 0 para 5Mbps.
	CPE(config-interface)#rate-limit { input | output } { access-group list | dscp dscp | qos-group qg } rate **Exemplo:** CPE(config-ethernet0)#rate-limit input dscp 10-46 12M	Configura limitação de taxa para determinados tráfegos na interface. Pode ser configurado no sentido de entrada (input) ou saída (output). **Parâmetros:** rate: taxa máxima permitida list: access-list para a qual se configura uma taxa máxima permitida dscp: valor de dscp para o qual se configura uma taxa máxima permitida qg: identificador do grupo para o qual se configura uma taxa máxima permitida O exemplo limita a taxa de entrada de pacotes de DSCP 10 (AF11) até DSCP 46 (EF) para 12Mbps.

Rate-Limit com Ações Diferenciadas

No Rate-Limit simples, os pacotes que excedem o limite são descartados. Já no com ações diferenciadas é possível configurar uma ação para os pacotes que excedem o limite e outra para os que não excedem. As ações podem ser transmitir, descartar ou remarcar. No Rate-Limit Simples o limite é composto apenas por uma taxa, mas no com ações diferenciadas o limite é na forma de um token bucket de dois parâmetros obrigatórios: taxa e rajada (burst). Observe a figura abaixo para entender melhor o funcionamento: os pacotes entram no tocken bucket e são classificados em 2 grupos, os que estão conformes e os que não estão. Cada grupo segue para uma ação, conform-action e exceed-action, respectivamente.



Abaixo estão listados os comandos para configurar.

Tabela 108: Configuração de Rate Limit com Ações Diferenciadas

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)#rate-limit { input | output } [access-group | dscp | qos-group] rate burst conform-action action exceed-action action **Exemplo:** CPE(config-ethernet0)#rate-limit output 5M 1k conform-action transmit exceed-action drop	Configura limitação de taxa para interface. Pode ser configurado no sentido de entrada (input) ou saída (output). **Parâmetros:** rate: taxa máxima permitida. burst: tamanho máximo de rajada permitida, em bytes. access-group: aplica o rate limit apenas sobre os pacotes da ACL. dscp: aplica o rate limite apenas sobre pacotes IP com DSCP escolhido. qos-group: aplica o rate limite apenas sobre pacotes IP com DSCP escolhido. **Action:** continue: busca por outros rate-limits na interface antes de ser transmitido drop: descartado set-cos: no caso de sair por vlan, define o CoS set-dscp: no caso de ser IP, define o DSCP set-qos: define o qos-group do pacote set-precedence: no caso de ser IP, define o Precedence set-tc: no caso de ser mpls, define o TC (antigo exp) transmit: transmite o pacote O exemplo limita a taxa de saída da interface ethernet 0 para 5Mbps com rajada de 1000 bytes, descartando pacotes que excedem e transmitindo pacotes que conformam

Traffic-Shape

Traffic-Shape é uma forma de conformação de tráfego. É criada uma limitação de taxa de saída em uma interface, assim como no policiamento. Entretanto, se a demanda de banda de saída daquela interface for maior do que a limitação, os pacotes vão sendo acumulados em um buffer e enviados assim que possível. Ressalta-se que esta disciplina é do tipo FIFO, não há reordenamento de pacotes. O que ocorre na prática é a suavização da curva da taxa de saída da interface. Abaixo estão listados os comandos para configurar Traffic-Shape.

Tabela 109: Configuração de QoS Traffic Shape

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)#traffic-shape rate Target bit rate **Exemplo:** CPE(config-ethernet0)#traffic-shape rate 10M	Configura conformação de tráfego para interface. **Parâmetros:** Target bit rate: taxa alvo para conformação de tráfego. O exemplo limita a taxa de saída da interface (Target bit rate) para 10Mbps. Se em um determinado momento a taxa necessária seja maior que esta, os pacotes são armazenados (até um limite de memória) e enviados quando a taxa necessária fique abaixo de Target bit rate.

4.10.5. Table-Map

Table Mapping é um mecanismo de marcação de pacotes extremamente flexível. A idéia básica é criar uma tabela de correspondências A ->B. Observe a tabela abaixo:

Entrada	Saída
0	1
1	1
5	2
7	2
Outros	5

Ao instalarmos esta tabela, um pacote que passar por ela e tiver marcado com 0, será marcado com 1. Outro pacote que estiver marcado com 1, continuará com 1. Os que entrarem com 5 ou 7 sairão com 2 e qualquer outro sairá com 5. Vamos a um exemplo real:

Tabela 110: Configuração de Table-Map

Passo	Comando	Objetivo
1	Digistar-CPE> enable	Habilita o usuário privilegiado.
2	Digistar-CPE# configure terminal	Acessa o modo de configuração.
3	Digistar-CPE(config)# table-map nome **Exemplo:** Digistar-CPE(config)# table-map exemplo	Acessa o modo de configuração da table-map **Parâmetros:** Nome: nome da tabela. O exemplo acessa o modo de configuração da table-map exemplo.
	Digistar-CPE(config-tablemap)#description texto	(Opcional) Configura uma descrição para a tabela **Parâmetros:** texto: descrição da tabela
	Digistar-CPE(config-tablemap)#map from from_value to to_value **Exemplo:** Digistar-CPE(config-tablemap)#map from 1 to 5	(Opcional) Mapeia um valor de entrada para um valor de saída. Repete-se este comando para quantas associações se queira fazer. **Parâmetros:** From_value: valor de entrada To_value: valor de saída O exemplo configura para que todos pacotes que entrarem com valor 1 saiam com 5.
	Digistar-CPE(config-tablemap)# default value **Exemplo:** Digistar-CPE(config-tablemap)# default 0	(Opcional) Configura um valor padrão de saída para valores de entrada não configurados. **Parâmetros:** value: valor de saída padrão. O exemplo configura o valor de saída padrão para 0.

A tabela configurada acima escreve 5 em todos os pacotes que entrarem com 1 e, para todos os que tiverem outro valor de entrada, escreve 0.

Mas ainda falta decidir quais os campos (Precedence, DSCP, COS, TC...) que esta tabela vai ler e escrever. Isto é feito na instalação da tabela no sentido de entrada da interface.

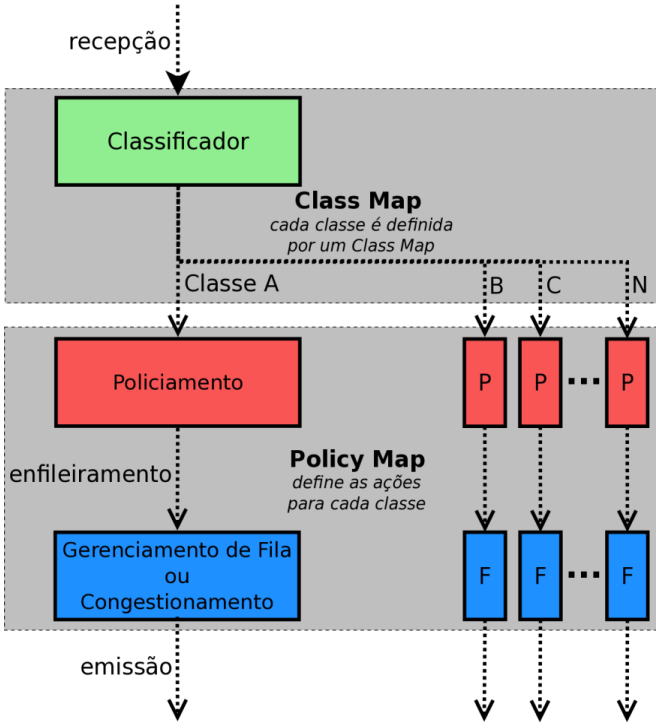
Tabela 111: Configuração de Table-Map na Interface

Passo	Comando	Objetivo
1	Digistar-CPE> enable	Habilita o usuário privilegiado.
2	Digistar-CPE# configure terminal	Acessa o modo de configuração.
3	Digistar-CPE (config)# interface type number **Exemplo:** Digistar-CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	Digistar-CPE(config-interface)#input table name to from **Exemplo:** Digistar-CPE(config-ethernet0)#input table examplo cos precedence	Configura a tabela para atuar na entrada da interface. **Parâmetros:** name: nome da tabela to: campo a ser escrito na saída from: campo a ser lido na entrada O exemplo configura a interface com a tabela exemplo do item anterior, lendo o campo COS e escrevendo no IP PRECEDENCE. Conforme configurado no item anterior, qualquer pacote que entrar com COS 1, sairá com IP PRECEDENCE 5. Qualquer outros valor de COS de entrada sairá com IP PRECEDENCE 0 (configuração de valor padrão de saída).

Este mecanismo ainda pode ser usado nas classes do Policy-Map de forma idêntica, como será mostrado mais adiante.

4.10.6. Traffic Policy

A configuração de Traffic Policies permite a criação de soluções de QoS específicas. Em um Traffic Policy o tráfego de interesse é classificado e organizado em conjuntos (Class Maps). Estes conjuntos são compostos basicamente por regras de admissão às quais o tráfego é submetido. Depois, para cada conjunto, são configuradas ações sobre o tráfego (um Policy Map). As ações podem ser de diferentes naturezas e também combinadas entre si para um mesmo Class Map. A figura abaixo mostra a relação entre Class Maps e Policy Maps, assim como o caminho dos pacotes de rede dentro de um Traffic Policy.



Uma Traffic Policy é descrita por apenas um ou por um conjunto de Policy Maps relacionados.

Na próxima sessão são explicadas as ações configuráveis para cada classe (definida por um Class Map) em um Policy Map e suas combinações possíveis.

Ações Suportadas

As ações suportadas pelo Policy Map são:

- Reserva de Largura de Banda: reserva-se uma fatia da largura de banda na interface para uma classe do Policy Map. A quantidade máxima reservável é limitada por max-res-bandwidth, presente na configuração da interface. (valor padrão 90%).

- Reserva de Largura de Banda com Priorização: reserva-se uma fatia da largura de banda na interface para uma classe. Além disso, o tráfego desta classe terá prioridade sobre as outras classes não prioritárias do Policy Map. A quantidade máxima reservável é limitada por max-res-bandwidth.

- Descarte de Pacotes: todos os pacotes da classe são descartados.

- Controle de Congestionamento: é possível habilitar os seguintes mecanismos para cada classe do Policy Map: WFQ e SFQ.

- Prevenção de Congestionamento: é possível habilitar os seguintes mecanismos para cada classe do Policy Map: WRED e SFB.

- Conformação de Tráfego: da mesma forma que é feita na interface, a conformação de tráfego está disponível para cada classe do Policy Map.

- Marcação de Pacotes: configura-se o Policy Map para que todo o tráfego pertencente a uma classe tenha seus pacotes modificados. Esta modificação pode ser nos seguintes campos: precedência IP, DSCP, MPLS Traffic Class e CoS.

- Encadeamento de Policy Maps: todo tráfego de uma classe de um Policy Map pode ser submetido a um novo Policy Map.

- Policiamento: configura-se o Policy Map para que todo o tráfego pertencente a uma classe seja submetido a restrições de banda antes de ser enfileirado, podendo ser remarcado ou até descartado.

Assim como na configuração de mecanismos QoS na interface, existem limitações das combinações de mecanismos QoS como ações nos Policy Maps. A tabela abaixo mostra as combinações possíveis:

Tabela 112: Combinações de Ações Possíveis para uma Classe de um Policy Map

	BW	PR	CC	CA	Conformação	Marcação	Policiamento	Encadeamento
BW	-	NÃO	SIM	SIM	SIM	SIM	SIM	SIM
PR	NÃO	-	SIM	SIM	SIM	SIM	SIM	SIM
CC	SIM	SIM	-	NÃO	SIM	SIM	SIM	NÃO
CA	SIM	SIM	NÃO	-	SIM	SIM	SIM	NÃO
Conformação	SIM	SIM	SIM	SIM	-	SIM	SIM	SIM
Marcação	SIM	SIM	SIM	SIM	SIM	-	SIM	SIM
Policiamento	SIM	SIM	SIM	SIM	SIM	SIM	-	SIM
Encadeamento	SIM	SIM	NÃO	NÃO	SIM	SIM	SIM	-

Observação: Descarte não pode ser combinado com nenhuma outra ação e policiamento pode ser combinado com todas.

BW = Reserva de Largura de Banda
PR = Reserva de Largura de Banda com Prioridade
CC = Controle de Congestionamento
CA = Prevenção de Congestionamento

Configuração

A configuração de Traffic Policies é feita em três passos obrigatórios: o primeiro consiste em classificar o tráfego, criando os conjuntos. Isto é feito pelo Class Map. Então, é necessário que se definam as ações para cada Class Map, isto é feito pela configuração do Policy Map. Por último, ativa-se um Policy Map em uma interface através do Service Policy, e dizemos que esta interface contém um Traffic Policy.

Configuração de um Class Map

Um Class Map representa um conjunto de tráfegos. Este conjunto possui um nome, uma descrição e uma série de regras que identificam um tráfego qualquer como pertencente ao conjunto. Um determinado tráfego só fará parte do conjunto do Class Map se satisfizer alguma (tipo match-any) ou todas (tipo match-all) as regras do Class Map. O nome de Class Map “class-default” é reservado e não pode ser usado neste ponto.

Tabela 113: Configuração de Class Map

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# class-map { match-any | match-all } WORD **Exemplo:** CPE (config)# class-map C1	Cria o Class Map de identificador WORD. **Parâmetros:** match-any: tráfego pertence ao conjunto ao satisfazer uma ou mais das regras. Match-all: tráfego pertence ao conjunto apenas ao satisfazer todas as regras. WORD: nome do Class Map **Atenção:** Caso match-any ou match-all sejam omitidos, o novo Class Map será do tipo match-all. O exemplo cria um Class Map de nome C1 do tipo match-all.
4	CPE (config-cmap)# description LINE **Exemplo:** CPE (config-cmap)# description esta e a descricao do C1	(Opcional) Atribui uma descrição LINE para o Class Map. **Parâmetros:** LINE: texto da descrição O exemplo configura o Class Map C1 com a descrição “esta e a descricao do C1”.

5	CPE (config-cmap)# match { access-group list | any | arp | interface type number | ip voip { sip | rtp } | **(apenas modelos com VoIP)** ipx | mpls { unicast | multicast | tc } | vlan { id | any | cos value } } **Exemplo:** CPE (config-cmap)# match ip precedence priority CPE (config-cmap)# match interface ethernet 1	Cria uma regra para que um determinado tráfego faça parte do conjunto de tráfegos do Class Map. **Regras e Parâmetros:** access-group: pacotes classificados pela access-list list satisfazem a regra any: todo tráfego satisfaz a regra arp, ipx: tráfego com estes protocolos sobre o protocolo de enlace satisfazem a regra. interface: tráfego vindo da interface type number satisfaz a regra ip voip: pacotes sip ou rtp satisfazem a regra. mpls: pacotes mpls com o campo TC especificado, unicast ou multicast satisfazem a regra. vlan id: pacotes vlan com tag id satisfazem a regra. vlan any: qualquer pacote de vlan satisfaz a regra. vlan cos value: pacotes vlan de cos value satisfazem a regra. O exemplo configura o Class Map C1 como conjunto de todo tráfego de precedência IP priority (1) e que também esteja entrando pela interface ethernet 1 (match-all).
	CPE (config-cmap)# show **Exemplo:** CPE (config-cmap)# show class-map C1 description esta e a descricao do c1 match ip precedence priority match interface ethernet 1 !	(Opcional) Mostra o resumo das configurações feitas. O exemplo mostra as configurações recém feitas neste Class Map.

Configuração de Largura de Banda Reservável

Esta configuração da interface é opcional para Traffic Policies e recomenda-se que não seja alterada sem fortes razões. O parâmetro max-reserved-bandwidth define a porcentagem máxima de banda reservável pelas classes do Traffic Policy a ser aplicado. Com o valor padrão de 75%, é possível reservar até 75% da largura de banda disponível na interface. Para alterar este valor, os comandos são mostrados abaixo.

Tabela 114: Configuração de Largura de Banda Reservável

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE (config-interface)# max-res-bandwidth percent **Exemplo:** CPE(config-ethernet0)# max-res-bandwidth 70	Altera a largura de banda reservável na interface. **Parâmetros:** percent: porcentagem da largura de banda da interface. O exemplo configura a interface ethernet0 com no máximo 70% de banda reservável.

Configuração de um Policy Map

Um Policy Map engloba diversos Class Maps e especifica o conjunto de ações a serem tomadas para cada classe. Se define, por exemplo, que o tráfego pertencente a uma determinada classe será tratado com controle de congestionamento e o tráfego de outra classe receberá apenas reserva de largura de banda. Podem ser configurados até 14 classes (Class Maps) em um único Policy Map.

Dentro de um Policy Map sempre existe uma classe padrão, chamada class-default. Nesta classe são classificados todos os pacotes que não pertencem a nenhuma das outras classes. É impossível remover esta classe.

Tabela 115: Configuração de Policy Map

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# policy-map WORD **Exemplo:** CPE (config)# policy-map P1	Cria um Policy Map de nome WORD. O exemplo cria um Policy Map de nome P1.
4	CPE (config-pmap)# description LINE **Exemplo:** CPE (config-pmap)# description acoes para C1	(Opcional) Atribui uma descrição LINE para o Policy Map. **Parâmetros:** LINE: texto da descrição O exemplo configura o Policy Map P1 com a descrição “acoes para C1”.
5	CPE (config-pmap)# class WORD **Exemplo:** CPE (config-pmap)# class C1	Entra no modo de configuração de ações para o Class Map WORD dentro do Policy Map. **Parâmetros:** WORD: texto da descrição O exemplo entra no modo de configuração das ações para o conjunto de tráfego C1.
6	CPE (config-pmap-c)# bandwidth { rate | percent percent | remaining percent } **Exemplo:** CPE(config-pmap-c)# bandwidth 25M	(Opcional) Configura o Class Map com reserva de largura de banda **Parâmetros:** rate: banda reservada percent: banda reservada como porcentagem percent da banda reservável. Remaining: banda reservada como porcentagem percent da banda reservável ainda não reservada (restante). O exemplo configura o Policy Map P1 para que o tráfego definido pelo Class Map C1 tenha no mínimo 25Mbps de banda disponível.

7	CPE (config-pmap-c)# priority { high | medium | low } { rate | percent percent } **Exemplo:** CPE(config-pmap-c)# priority high 15M	(Opcional) Configura o Class Map com reserva de largura de banda e prioridade sobre outros tráfegos. **Parâmetros:** rate: banda reservada percent: banda reservada como porcentagem percent da banda reservável. high, medium, low: classes high terão menor latência que Medium, que terão menor latência que as configuradas com o comando Bandwidth, que terão menor latência que as de prioridade Low. O exemplo configura o Policy Map P1 para que o tráfego definido pelo Class Map C1 tenha no mínimo 15Mbps de banda disponível e tenha prioridade máxima dentro do Policy Map P1.
8	CPE (config-pmap-c)# drop **Exemplo:** CPE (config-pmap-c)# drop	(Opcional) Configura o Policy Map para que descarte todos pacotes pertencentes ao Class Map.
9	CPE (config-pmap-c)# fair-queue **Exemplo:** CPE (config-pmap-c)# fair-queue	(Opcional) Configura o Policy Map P1 para que todo tráfego pertencente ao conjunto do Class Map C1 seja encaminhado de acordo com o mecanismo de controle de congestionamento Weighted Fair Queueing (WFQ).
10	CPE (config-pmap-c)# random-detect { prec-based | dscp-based } **Exemplo:** CPE (config-pmap-c)# random-detect prec-based	(Opcional) Configura o Policy Map P1 para que todo tráfego pertencente ao conjunto do Class Map C1 seja encaminhado de acordo com o mecanismo de prevenção de congestionamento Weighted Random Detect (WRED). **Parâmetros:** prec-based: a WRED tem 8 curvas distintas para as 8 precedências IP. Dscp-based: a WRED tem 64 curvas distintas para os 64 valores de DSCP. O exemplo configura C1 com uma WRED por precedência IP.
11	CPE (config-pmap-c)# sto-fair-queue **Exemplo:** CPE (config-pmap-c)# sto-fair-queue	(Opcional) Configura o Policy Map P1 para que todo tráfego pertencente ao conjunto do Class Map C1 seja encaminhado de acordo com o mecanismo de controle de congestionamento Stochastic Fair Queueing (SFQ).
12	CPE (config-pmap-c)# sto-fair-blue **Exemplo:** CPE (config-pmap-c)# sto-fair-blue	(Opcional) Configura o Policy Map P1 para que todo tráfego pertencente ao conjunto do Class Map C1 seja encaminhado de acordo com o mecanismo de prevenção de congestionamento Stochastic Fair Blue (SFB).

13	CPE (config-pmap-c)# shape rate rate **Exemplo:** CPE (config-pmap-c)# shape rate 1M	(Opcional) Configura o Class Map para conformação de tráfego. **Parâmetros:** rate: taxa limite alvo da conformação de tráfego. O exemplo configura o Policy Map P1 para que o tráfego definido pelo Class Map C1 seja conformado para 1Mbit.
14	CPE (config-pmap-c)# set { cos cos | precedence prec | dscp dscp | mpls traffic-class tc | qos-group group } **Exemplo:** CPE(config-pmap-c)#set ip precedence flash-override	(Opcional) Configura o Policy Map para que todo o tráfego pertencente ao Class Map seja marcado (sinalização) com algum atributo. No caso de dscp e precedence, a marcação é feita para ambas versões suportadas do protocolo IP. **Parâmetros:** cos: atribui o valor cos no campo correspontente do quadro ethernet. ip prec: substitui o valor da precedência IP dos pacotes para prec ip dscp: substitui o valor DSCP dos pacotes para dscp mpls traffic-class: configura os bits mpls traffic-class com o valor tc (antigos exp bits). qos-group: índice do grupo que o pacote deve pertencer ao passar pela política. O exemplo configura o Policy Map P1 para que o tráfego definido pelo Class Map C1 tenha precedência ip flash-override
15	CPE(config-pmap-c)# service-policy WORD **Exemplo:** CPE(config-pmap-c)# service-policy P2	(Opcional) Configura o Policy Map para que o tráfego do Class Map seja submetido às regras de admissão dos Class Maps de outro Policy Map e, caso as satisfaça, seja submetido às suas ações. O tráfego não admitido não está sujeito às ações do outro Policy Map. É permitido no máximo dois encadeamentos de Policy Maps. **Parâmetros:** WORD: nome do Policy Map O exemplo configura o Policy Map P1 para que o tráfego definido pelo Class Map C1 seja submetido às regras e ações do Policy Map P2.

16	CPE (config-cmap-c)# show
	
	Exemplo:
	CPE (config-pmap-c)# show
	class C1
	  bandwidth 25000
	  sto-fair-queue
	  set ip precedence flash-override
	!
		(Opcional) Mostra o resumo das configurações feitas no Class Map.
		
		O exemplo mostra as configurações recém feitas neste Class Map do Policy Map.

17	CPE (config-cmap-c)# exit	(Opcional) Sai do modo de configuração do Class Map e volta para a configuração do Policy Map.
18	CPE (config-pmap)# show **Exemplo:** CPE (config-pmap)# show policy-map P1 class C1 bandwidth 25000 sto-fair-queue set ip precedence flash-override ! class class-default ! !	(Opcional) Mostra o resumo das configurações feitas no Class Map O exemplo mostra as configurações recém feitas neste Policy Map. Como só existe um Class Map configurado, é mostrado apenas o C1.

Configuração de Policiamento em um Policy Map

A configuração de policiamento em cada classe de um Policy Map permite que se policiem os pacotes a serem enfileirados nas filas da classe. Este policiamento é feito do modo "2 taxas 3 cores", descrito na RFC2698, ou do modo "1 taxa 3 cores" descrito na RFC2697.

Para entender como funciona, observe a figura abaixo: os pacotes entram no primeiro token buket (TB), configurado com uma taxa e uma rajada (opcional), caso não estejam conformes, a ação violate-action é aplicada sobre eles. Já os que estão conformes, seguem para um segundo TB. Neste segundo, configurado também com uma taxa obrigatória e uma rajada opcional, os pacotes não conformes têm a ação exceed-action aplicada sobre eles. Nos conformes são aplicados a ação conform-action. A taxa do primeiro TB é chamada de PIR (Peak Information Rate) e sua rajada de BE (Burst Excess). Já no segundo são chamados de CIR (Commited Information Rate) e BC (Burst Conform). No caso da RFC2697, CIR e PIR possuem o mesmo valor e BE > BC.

É importante ressaltar que tudo isto ocorre antes dos pacotes da classe serem enfileirados e estarem sujeitos às ações do policy-map.

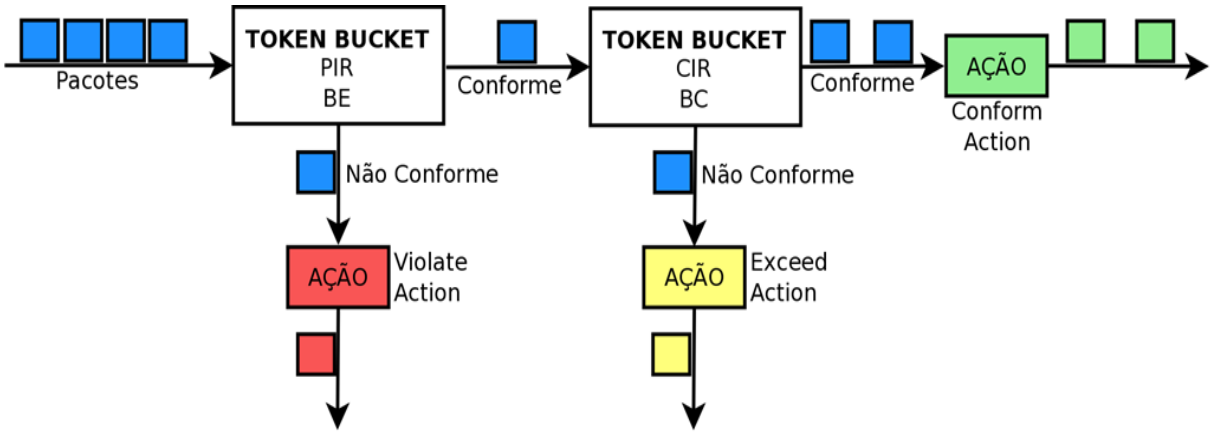


Tabela 116: Configuração de Policiamento em um Policy Map

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# policy-map WORD **Exemplo:** CPE (config)# policy-map P1	Cria ou entra em um Policy Map de nome WORD. O exemplo entra no Policy Map de nome P1 criado anteriormente.
4	CPE (config-pmap-c)# police [cir] cir [bc] bc [pir pir] [be] be **Exemplo:** CPE (config-pmap-c)# Police cir 1M bc 500 pir 2M be 750	Configura policiamento para a classe e entra no modo de configuração das ações. **Parâmetros:** cir: taxa do primeiro TB. bc: tamanho de rajada (bytes) do primeiro pir (opcional): taxa do primeiro TB. Caso omito habilita o modo "1 taxa 3 cores", caso contrário habilita o modo "2 taxas 3 cores". be: tamanho de rajada (bytes) do segundo TB O exemplo configura policiamento de acordo com a RFC2698 e entra no modo de configuração das ações.
5	CPE (config-pmap-c-police)# {violate-action | exceed-action | conform action} action **Exemplo:** CPE (config-pmap-c-police)# conform-action transmit CPE (config-pmap-c-police)# exceed-action set-dscp default CPE (config-pmap-c-police)# violate-action drop	Configura as ações para cada cor. **Action:** continue: busca por outros rate-limits na interface antes de ser transmitido drop: descartado set-cos: no caso de sair por vlan, define o CoS set-dscp: no caso de ser IP, define o DSCP set-precedence: no caso de ser IP, define o Precedence set-tc: no caso de ser mpls, define o TC (antigo exp) transmit: transmite o pacote set-qos: define um novo índice de grupo para o pacote O exemplo configura o policiador para transmitir pacotes verdes, remarcar pacotes amarelos com DSCP 0 e descartar pacotes vermelhos.

Configuração de um Service Policy

Configurados os Class Maps e Policy Maps, falta ainda ativar os Policy Maps nas interfaces. No caso de Policy Maps encadeados, é necessário que se ative apenas o Policy Map raíz, os outros serão ativados automaticamente.

Tabela 117: Configuração de Service Policy

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number **Exemplo:** CPE (config)# interface ethernet 0	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 0.
4	CPE(config-interface)# service-policy { input | output } WORD **Exemplo:** CPE(config-ethernet0)# service-policy P1	Ativa o Policy Map na interface, no sentido de saída ou entrada. **Parâmetros:** WORD: nome do Policy Map a ser ativado na interface. input: Policy Map é instalado para o tráfego que entra pela interface. output: Policy Map é instalado para o tráfego que sai pela interface. O exemplo ativa o Policy Map P1 na interface ethernet 0.

Exemplo de Traffic Policy

Conforme o diagrama abaixo, todo tráfego é dividido em três classes distintas: EMAIL, APLICAÇÕES e HTTP. Para cada classe é configurada uma reserva de largura de banda. Ressalta-se que esta reserva é o mínimo garantido. Caso, em um certo momento, uma classe esteja subutilizando sua banda reservada, outras classes podem fazer uso dela. Mas assim que a cedente necessitar de sua banda, as outras classes a devolvem imediatamente.

Para cada uma destas classes também são configuradas outras ações além da reserva. No caso da classe EMAIL, é ativado o controle de congestionamento SFQ, que trata de forma justa todos os fluxos. Para a classe APLICAÇÃO, todo tráfego é marcado com precedência IP 3. Já para a classe HTTP, todo tráfego é marcado com DSCP 0.

Uma das ações aplicadas à classe HTTP é um encadeamento de Policy Map. O Policy Map HTTP é encadeado na classe HTTP do Policy Map TESTE através do comando service-policy. Este novo Policy Map HTTP possui duas classes: PRIORITY e BULK, cada uma com as suas ações. Note que a classe HTTP engloba o as regras (e o tráfego) das classes PRIORITY e BULK juntas!

Algo muito semelhante se sucede na classe APLICAÇÕES, onde um Policy Map APLICAÇÕES é encadeado. A diferença é que na classe ORACLE do Policy Map APLICAÇÕES, um novo Policy Map ORACLE é encadeado, que contém duas classes: GOLD e SILVER. O nível máximo de encadeamentos é atingido (2).

A configuração dos Class Maps envolvidos é mostrada a seguir e, logo após, a configuração dos Policy Maps utilizados também é mostrada:

```
class-map match-any EMAIL
  description "Portas 3000 a 3001"
  match ip protocol udp sport eq 3001
  match ip protocol udp sport eq 3000
!
class-map match-any APLICACOES
  description "Portas 3002 a 3009"
  match ip protocol udp sport eq 3002
  match ip protocol udp sport eq 3003
  match ip protocol udp sport eq 3004

  match ip protocol udp sport eq 3005
  match ip protocol udp sport eq 3006
  match ip protocol udp sport eq 3007
  match ip protocol udp sport eq 3008
  match ip protocol udp sport eq 3009
!
class-map match-any SAP
  description "Portas 3002 a 3003"
  match ip protocol udp sport eq 3002
  match ip protocol udp sport eq 3003
!
class-map PRIORITY
  description "Porta 3012"
  match ip protocol udp sport eq 3012
!
class-map match-any HTTP
  description "Portas 3010 a 3012"
  match ip protocol udp sport eq 3010
  match ip protocol udp sport eq 3011
  match ip protocol udp sport eq 3012
!
```

```
class-map match-any ORACLE
  description "Portas 3004 a 3009"
  match ip protocol udp sport eq 3004
  match ip protocol udp sport eq 3005
  match ip protocol udp sport eq 3006
  match ip protocol udp sport eq 3007
  match ip protocol udp sport eq 3008
  match ip protocol udp sport eq 3009
!
class-map match-any GOLD
  description "Portas 3004 a 3005"
  match ip protocol udp sport eq 3004
  match ip protocol udp sport eq 3005
!
class-map match-any SILVER
  description "Portas 3006 a 3008"
  match ip protocol udp sport eq 3006
  match ip protocol udp sport eq 3007
  match ip protocol udp sport eq 3008
!
class-map match-any BULK
  description "Portas 3010 a 3011"
  match ip protocol udp sport eq 3010
  match ip protocol udp sport eq 3011
!
```

-X-

```
policy-map ORACLE
  class GOLD
    priority medium 2000
    random-detect prec-based
  !
  class SILVER
    bandwidth 1000
    fair-queue
  !
!
policy-map APLICACOES
  class SAP
    bandwidth 1500
    sto-fair-blue
  !
  class ORACLE
    bandwidth 3000
    service-policy ORACLE
```

```
 !
!
policy-map HTTP
 class BULK
  bandwidth 2000
  sto-fair-queue
 !
 class PRIORITY
  priority high 300
 !
!
policy-map TESTE
 class EMAIL
  bandwidth 500
  sto-fair-queue

 !
 class APLICACOES
  bandwidth 4500
  service-policy APLICACOES
  set ip precedence 3
 !
 class HTTP
  bandwidth 5000
  service-policy HTTP
  set ip dscp 0
 !
!
```

4.10.6.1. Estatísticas de QoS

É possível obter informações sobre o comportamento das filas dos mecanismos de QoS Controle de Congestionamento e Prevenção de Congestionamento nas interfaces. Os dados mostrados são bytes enviados, pacotes enviados e descartados, sendo por fila, fluxo ou classe quando aplicável.

Tabela 118: Obtenção de Estatísticas das Filas QoS

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# show queueing [custom | fair | interface type number | priority | random-detect] **Exemplo 1:** digistar#show queueing interface ethernet 1 Interface ethernet1 queueing strategy: fifo Output queue: 2790494/42377/0 (bytes/packets/dropped)	Mostra estatísticas de QoS **Parâmetros (opcionais):** custom: mostra apenas estatísticas das interfaces configuradas com CQ. fair: mostra apenas estatísticas das interfaces configuradas com WFQ. interface: mostra apenas estatísticas da interfaces type number. priority: mostra apenas estatísticas das interfaces configuradas com PQ. random-detect: mostra apenas estatísticas das interfaces configuradas com WRED. O exemplo 1 mostra o comando que exibe as estatísticas da fila da interface ethernet 1.

Para mostrar estatísticas sobre o Traffic Policies, utiliza-se o comando **show service-policy** interface.

```
digistar#show service-policy interface ethernet 0
service-policy output example
 class          res. bandwidth  packets sent  packets dropped          traffic  conform/exceed/violate pkts
  gold             5000Kbit          192                0  912Kbit/121pps        policer not configured
  silver          15000Kbit          233                0    13Kbit/31pps        policer not configured
  bronze          40000Kbit         1487                3  1892Kbit/210pps               1480/4/3
  class-default    1000Kbit            5                1       0Kbit/0pps        policer not configured
```

4.11. Túneis

O roteador suporta diversos tipos de tunelamento IP. Cria-se uma interface virtual chamada *tunnel* que possui parâmetros extras de configuração relativos ao túnel. Outros comandos também estão disponíveis nesta interface (QoS, Multicast...) e podem ser utilizado normalmente, mas eles apenas serão ativados após o túnel ser corretamente configurado.

Para ajudar na configuração do túnel, dentro da interface virtual *tunnel* existe o comando "check-configuration". Este comando irá verificar se todas as configurações necessárias para o funcionamento do túnel foram feitas e exibir mensagens para auxiliar a configuração ou depuração.

Os seguintes modos são suportados:

- 6rd: IPv6 Rapid-Deployment Tunnelig
- 6to4: Ipv6 Automatic Tunnelling
- greip: Generic Route Encapsulation Protocol over IP
- ip6: Generic Encapsulation over IPv6
- ip6ip: IPv6 sobre IPv4
- ip6ip6: IPv6 sobre IPv6
- ipip: IPv4 sobre IPv4
- isatap: IPv6 Automatic Tunneling

Para configurar um túnel, basta seguir os comandos abaixo. Neste exemplo configuraremos um túnel que terá seus pacotes transitando da seguinte forma.

Aplicação
Transporte
IP (10.1.1.1 ↔ 10.1.1.0/24)
GRE
IP (192.168.11.1 ↔ 192.168.11.2)
Enlace
...

Tabela 119: Configuração de Tunelamento

Passo	Comando	Objetivo
1	Digistar-CPE> enable	Habilita o usuário privilegiado.
2	Digistar-CPE# configure terminal	Acessa o modo de configuração.
3	Digistar-CPE (config)# interface tunnel number **Exemplo:** Digistar-CPE (config)# interface tunnel 0	Acessa o modo de configuração da interface. O exemplo cria a interface virtual *tunnel 0* e acessa seu modo de configuração.
4	Digistar-CPE(config-tunnel0)# tunnel mode mode **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel mode greip	Esta configuração é obrigatória e todos os passos abaixo são obrigatórios, opcionais ou não disponíveis de acordo com o modo selecionado. Observe a tabela mais abaixo para ver a relação entre os modos e os comandos. A marcação de opcional ou obrigatório dos próximos passos é uma generalização. **Parâmetros:** mode: modo do túnel (ipip, greip...) O exemplo configura o modo para greip
	Digistar-CPE(config-tunnel0)# tunnel checksum	(Opcional, indisponível dependo do modo) Habilita Checksumming dos pacotes
5	Digistar-CPE(config-tunnel0)# tunnel destination { addr | addr6 } **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel destination 192.168.11.1	Configura o Destino do Túnel **Parâmetros:** addr: endereço IPv4 de destino do túnel. Usado quando se encapsula algo sobre IPv4. Addr6: endereço IPv6 de destino do túnel. Usado quando se encapsula algo sobre IPv6. O exemplo configura destino 192.168.11.1 para o nosso túnel do tipo greip.
	Digistar-CPE(config-tunnel0)# tunnel key key	(Opcional, indisponível dependo do modo Configura Chave de Seleção **Parâmetros:** key: chave de seleção
	Digistar-CPE(config-tunnel0)# tunnel sequence-datagrams	(Opcional, indisponível dependo do modo Descarta Pacotes fora de Sequêcia

	Digistar-CPE(config-tunnel0)# tunnel source { addr | addr6 } **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel destination 192.168.11.2	(Opcional) Configura a Origem do Túnel **Parâmetros:** addr: endereço IPv4 de origem do túnel. Usado quando se encapsula algo sobre IPv4. Addr6: endereço IPv6 de origem do túnel. Usado quando se encapsula algo sobre IPv6. O exemplo configura origem 192.168.11.2 para o nosso túnel do tipo greip.
	Digistar-CPE(config-tunnel0)# tunnel tos tos **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel tos 32	(Opcional) Configura o ToS dos pacotes do Túnel **Parâmetros:** tos: Type-of-Service O exemplo configura para que os pacotes do túnel tenham ToS 32.
	Digistar-CPE(config-tunnel0)# tunnel ttl ttl **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel ttl 255	(Opcional)Configura o TTL dos pacotes do Túnel **Parâmetros:** ttl: Time-to-Live O exemplo configura para que os pacotes do túnel tenham TTL 255.
	Digistar-CPE(config-tunnel0)#keepalive period count **Exemplo:** Digistar-CPE(config-tunnel0)# keepalive 10 10	(Opcional para GREIP) Habilita o mecanismo de Keepalive. **Parâmetros:** period: intervalo entre cada envio de keepalive count: número de respostas perdidas até que o túnel seja considerado inativo. **Observação:** a resposta de keepalives está sempre habilitada para túneis do tipo GREIP. O exemplo configura Keepalive com period de 10s e count de 10. Ou seja, a cada 10s é enviado um keepalive para o destino. Se 10 não forem respondidos em sequência, a interface tunnel é considerada **NOT RUNNING**.
6	Digistar-CPE(config-tunnel0)# tunnel address addr **Exemplo:** Digistar-CPE(config-tunnel0)# tunnel address 10.1.1.1/24	Configura um endereço para a interface túnel. Este endereço será encapsulado no túnel. Portanto, se estivermos encapsulando IPv6 sobre IPv4, aqui vai o endereço IPv6 da interface túnel e nos parâmetros do túnel (acima), vão os endereços IPv4 da camada encapsuladora. **Parâmetros:** addr: Endereço IPv4/IPv6 da interface túnel. O exemplo configura o endereço do túnel como 10.1.1.1.
7	Digistar-CPE(config-tunnel0)# no shutdown	Configura a interface para rodar

A relação entre os parâmetros do túnel e os modos, é a seguinte:

Modo/ Comando	6rd	6to4	greip	ip6	ip6ip	ip6ip6	ipip	isatap
Checksum	O	O	O	U	O	U	O	O
Destination	M	U	O	O	O	O	O	U
Key	U	U	O	U	U	U	U	U
Sequence	O	O	O	U	O	U	O	O
Source	M	M	O	O	O	O	O	M
ToS	O	O	O	O	O	O	O	O
TTL	O	O	O	O	O	O	O	O
Keepalive	U	U	O	U	U	U	U	U

O = Opcional, M = Obrigatório, U = Indisponível

4.12. IP Service Level Agreement (IP SLA)

(recurso habilitado por licença)

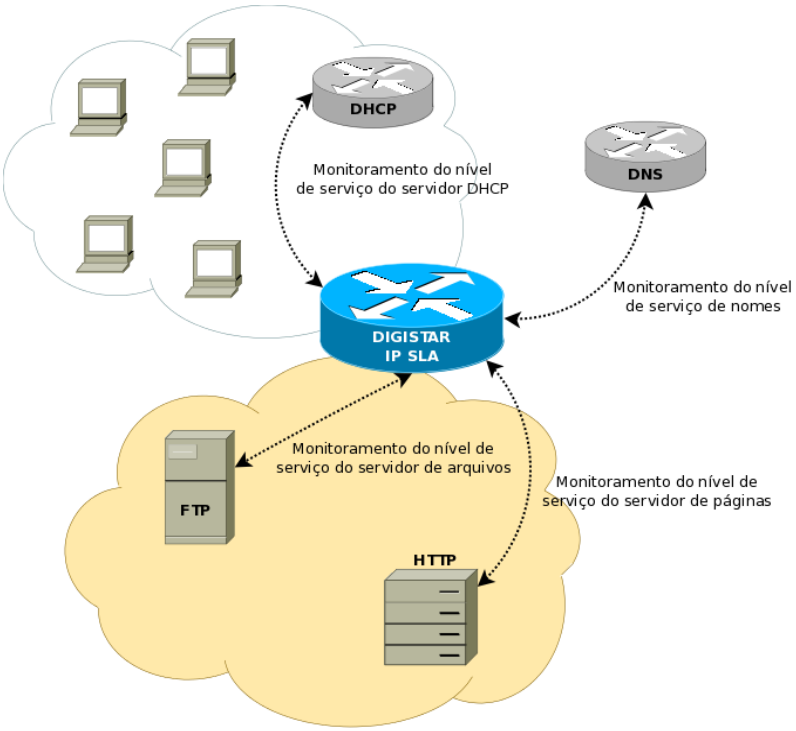
IP SLA é uma ferramenta capaz de analisar os níveis de serviços de aplicações e redes IP, contribuindo para o bom funcionamento destes, aumentando a produtividade e diminuindo custos operacionais.

Esta ferramenta realiza o monitoramento ativo dos serviços, ou seja, ela de fato injeta pacotes na rede com o objetivo de medir o serviço prestado, de forma continua, previsível e confiável. Assim é possível medir e prover acordos de nível de serviço, além de ajudar no melhor entendimento do desempenho da rede, facilita a instalação de novos serviços, verifica implementações de QoS e ainda ajuda administradores de rede na investigação de problemas.

O monitoramento de um serviço relacionado a uma certa entidade de rede é feito por um IP SLA Monitor. Ele realiza operações com o intuito de coletar estatísticas sobre o nível de serviço prestado por ela. Dependendo do serviço a ser analisado, o tipo correto de operação realizada pelo monitor deve ser escolhido.

A figura abaixo mostra o uso de quatro IP SLA Monitors para monitorar os níveis de serviço prestados por um servidor de arquivos FTP, outro de páginas web, um de nomes e também outro de DHCP.

No caso do monitor FTP, são coletadas estatísticas sobre cada operação de download de arquivos, realizada regularmente. Para o servidor de páginas web, é medido o tempo descarga de uma página html. Para o servidor DHCP, são feitas tentativas de se obter um endereço IP onde o tempo de resposta é medido. E, por último, o tempo de resposta do servidor DNS é medido, através de requisições de resolução de nomes.



Na próxima seção são mostradas as operações suportadas pelos IP SLA Monitors.

4.12.1. Visão Geral das Operações Suportadas

O IP SLA suporta basicamente dois grupos de operações: SLAs de rede e SLAs de aplicação. Os SLAs de rede são responsáveis por medir o serviço da camada de rede, através de, por exemplo, resolução de endereços. Já os SLAs de aplicação tem o objetivo de medir os níveis de serviço de aplicações, como, por exemplo, um servidor de páginas web.

Entre os SLAs de rede, as seguintes operações são suportadas:

- DHCP Client: mede o tempo de resposta para se obter um endereço IP através do servidor DHCP da rede conectada em uma interface.

- DNS Query: permite medir a diferença de tempo entre mandar uma requisição DNS e receber a resposta.

- Echo: também conhecida como ping, esta operação permite medir o tempo de resposta fim a fim da rede.

- Path Discovered Echo: também conhecida como traceroute, permite medir o tempo de resposta fim a fim ou salto por salto da rede, identificando os pontos críticos.

- TCP Echo: definido na RFC 862, mede o tempo de iniciar uma conexão TCP, enviar dados e recebê-los de volta.

- UDP Echo: definido na RFC 862, mede o tempo de enviar dados e recebê-los de volta, via UDP.

Entre os SLAs de aplicação, as seguintes operações são suportadas:

- FTP: permite medir o tempo gasto para baixar um arquivo de um servidor FTP.
- HTTP: permite medir o tempo gasto para baixar uma página web de um servidor HTTP.

Na próxima seção será mostrado como configurar IP SLAs.

4.12.2. Configuração de IP SLAs

A configuração de IP SLAs é feita basicamente em dois passos. Primeiro deve-se criar e configurar um IP SLA Monitor. Neste passo, escolhe-se o tipo de serviço a ser monitorado e ajusta-se parâmetros que reflitam melhor as características do monitoramento a ser realizado. No segundo passo, ativa-se o monitor (e suas operações). Nesta ativação configura-se o horário de início, duração e recorrência das operações do monitor.

4.12.2.1. Configuração de Monitores

Existem algumas configurações comuns e opcionais à todos tipos de operações. São elas:

- Descrição: é possível adicionar uma breve descrição para cada monitor. Por exemplo: “monitor echo do gateway”.
- Frequência: configura o tempo entre cada repetição de operação do monitor. O valor padrão, caso não configurado, é de 60 segundos entre uma operação e outra. Por exemplo, no caso de uma operação Echo (ping), um icmp ping request será enviado a cada 60 segundos.
- Timeout: tempo que cada operação pode levar até ser considerada como falha. Por exemplo, numa operação Echo (ping), se um icmp ping reply não voltar em um certo tempo, a operação será considerada falha. O valor padrão deste tempo é 5000ms (5 segundos).

- Horas de estatísticas guardadas: este parâmetro é muito importante e, embora opcional, deve receber um valor adequado para a finalidade do monitor. Ele especifica por quantas horas os resultados de cada operação devem ser guardados. O valor padrão é 6 horas. Por exemplo, após a execução de um Echo (ping), as estatísticas desta operação ficarão disponíveis até 6 horas após sua execução.

Algumas operações possuem as seguintes configurações opcionais, com os seguintes valores padrão:

- Type of Service (ToS): 0
- Tamanho da carga payload: 56 bytes
- Time to Live (TTL): 255

Operação DHCP Client

A operação DHCP Client mede o tempo necessário para se obter um endereço IP na rede de uma determinada interface. É necessário configurar a interface que será feita esta operação.

Tabela 120: Configuração de IP SLA DHCP Client

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 1	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# typedhcp interface ethernet number **Exemplo:** CPE(config-sla-monitor)# typedhcp interface ethernet 1	Configura a operação do monitor para ser do tipo DHCP Client. **Parâmetros:** *number*: número da interface na qual se deseja realizar a operação O exemplo configura a operação para ser do tipo DHCP na interface ethernet 1.
5	CPE(config-sla-monitor-dhcp)# description text **Exemplo:** CPE(config-sla-monitor-dhcp)# description DHCP na ethernet 1	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** *text:* texto que descreve a operação O exemplo configura a monitor com a descrição “DHCP na ethernet 1”
	CPE(config-sla-monitor-dhcp)# frequency secs **Exemplo:** CPE(config-sla-monitor-dhcp)# frequency 3600	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 3600 segundos.
	CPE (config-sla-monitor-dhcp)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-dhcp)# hours-of-statistics-kept 72	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 72 horas.

	CPE (config-sla-monitor-dhcp)# timeout ms **Exemplo:** CPE(config-sla-monitor-dhcp)# timeout 5000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 5000 milissegundos (5 segundos).

Operação Echo

Esta operação envia icmp echo requests e espera icmp echo replies de volta. É necessário configurar o endereço de destino destes pings. Opcionalmente, pode-se configurar valores de Time to Live (TTL), Type of Serivice (ToS), tamanho do pacote icmp e endereço IP de origem.

Tabela 121: Configuração de IP SLA Echo

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 2	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# typeecho protocol ipicmpecho destination **Exemplo:** CPE(config-sla-monitor)# typeecho protocol ipicmpecho 192.168.11.1	Configura a operação do monitor para ser do tipo Echo. **Parâmetros:** destination: endereço IP de destino O exemplo configura a operação para ser do tipo echo com destino 192.168.11.1.
5	CPE(config-sla-monitor-echo)# description text **Exemplo:** CPE(config-sla-monitor-echo)# description echo no gateway	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição “echo no gateway”
	CPE(config-sla-monitor-echo)# frequency secs **Exemplo:** CPE(config-sla-monitor-echo)# frequency 30	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 30 segundos.

	CPE (config-sla-monitor-echo)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-echo)# hours-of-statistics-kept 24	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 24 horas.
	CPE (config-sla-monitor-echo)# timeout ms **Exemplo:** CPE(config-sla-monitor-echo)# timeout 5000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 5000 milissegundos (5 segundos).
	CPE (config-sla-monitor-echo)# size size **Exemplo:** CPE(config-sla-monitor-echo)# size 100	(Opcional) Configura o tamanho dos pacotes enviados pela operação. **Parâmetros:** size: tamanho do pacote em bytes O exemplo configura as operações com pacotes de 100 bytes.
	CPE (config-sla-monitor-echo)#source-ipaddr addr **Exemplo:** CPE(config-sla-monitor-echo)#source-ipaddr 192.168.5.5	(Opcional) Configura o endereço IP de origem dos pacotes enviados pela operação. **Parâmetros:** addr: endereço IP O exemplo configura os pacotes da operação com endereço IP de origem 192.168.5.5
	CPE (config-sla-monitor-echo)#tos value **Exemplo:** CPE(config-sla-monitor-echo)# tos 13	(Opcional) Configura o Type of Service dos pacotes enviados pela operação. **Parâmetros:** value: valor do ToS O exemplo configura os pacotes com ToS 13
	CPE (config-sla-monitor-echo)#ttl value **Exemplo:** CPE(config-sla-monitor-echo)#ttl 5	(Opcional) Configura o Time-to-Live dos pacotes enviados pela operação. **Parâmetros:** value: valor do ttl O exemplo configura os pacotes com TTL 5.

Operação FTP

Esta operação mede o tempo para buscar e baixar um arquivo de um servidor FTP. É necessário entrar com a URL do arquivo.

Tabela 122: Configuração de IP SLA FTP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 3	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# type ftp operation get url URL **Exemplo:** CPE(config-sla-monitor)# typeftp operation get url ftp://ftp.br.debian.org/debian/README.html	Configura a operação do monitor para ser do tipo FTP. **Parâmetros:** URL: url do arquivo a ser transferido O exemplo configura a operação para ser do tipo ftp, transferindo o arquivo README.html
5	CPE(config-sla-monitor-ftp)# description text **Exemplo:** CPE(config-sla-monitor-ftp)# description readme do debian	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição “readme do debian”
	CPE(config-sla-monitor-ftp)# frequency secs **Exemplo:** CPE(config-sla-monitor-ftp)# frequency 300	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 300 segundos.
	CPE (config-sla-monitor-ftp)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-ftp)# hours-of-statistics-kept 8	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 8 horas.

	CPE (config-sla-monitor-ftp)# timeout ms **Exemplo:** CPE(config-sla-monitor-ftp)# timeout 3000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 3000 milissegundos (3 segundos).

Operação HTTP

Esta operação mede o tempo para buscar e baixar uma página web de um servidor HTTP. É necessário entrar com a URL da página.

Tabela 123: Configuração de IP SLA HTTP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 4	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# type http operation get url URL **Exemplo:** CPE(config-sla-monitor)# typehttp operation get url http://sheldonbrown.com/web_sample1.html	Configura a operação do monitor para ser do tipo HTTP. **Parâmetros:** URL: url do arquivo a ser transferido O exemplo configura a operação para ser do tipo http, transferindo o arquivo web_sample1.html
5	CPE(config-sla-monitor-http)# description text **Exemplo:** CPE(config-sla-monitor-http)# description website exemplo	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição “website exemplo”
	CPE(config-sla-monitor-http)# frequency secs **Exemplo:** CPE(config-sla-monitor-http)# frequency 600	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 600 segundos.

	CPE (config-sla-monitor-http)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-http)# hours-of-statistics-kept 12	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 12 horas.
	CPE (config-sla-monitor-http)# timeout ms **Exemplo:** CPE(config-sla-monitor-http)# timeout 6000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 6000 milissegundos (6 segundos).

Operação Path Discovered Echo

Mede os tempos de resposta fim a fim e salto por salto até o destino. É necessário configurar o destino da medição. Opcionalmente, pode-se configurar o endereço IP de origem e o campo Type of Service (ToS) dos pacotes enviados.

Tabela 124: Configuração de IP SLA Path Discovered Echo

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 5	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# type pathecho protocol ipicmpecho destination **Exemplo:** CPE(config-sla-monitor)# type pathecho protocol ipicmpecho 192.168.11.1	Configura a operação do monitor para ser do tipo Path Discovered Echo. **Parâmetros:** destination: endereço IP de destino O exemplo configura a operação para ser do tipo pathecho com destino 192.168.11.1

5	CPE(config-sla-monitor-pathEcho)# description text **Exemplo:** CPE(config-sla-monitor-pathEcho)# description traceroute 10.15.14.13	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição "traceroute 10.15.14.13"
	CPE(config-sla-monitor-pathEcho)# frequency secs **Exemplo:** CPE(config-sla-monitor-pathEcho)# frequency 90	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 90 segundos.
	CPE (config-sla-monitor-pathEcho)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-pathEcho)# hours-of-statistics-kept 5	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 5 horas.
	CPE (config-sla-monitor-pathEcho)# timeout ms **Exemplo:** CPE(config-sla-monitor-pathEcho)# timeout 15000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 15000 milissegundos (15 segundos).
	CPE (config-sla-monitor-pathEcho)#source-ipaddr addr **Exemplo:** CPE(config-sla-monitor-pathEcho)#source-ipaddr 192.168.11.233	(Opcional) Configura o endereço IP de origem dos pacotes enviados pela operação. **Parâmetros:** addr: endereço IP O exemplo configura os pacotes da operação com endereço IP de origem 192.168.11.233
	CPE (config-sla-monitor-pathEcho)#tos value **Exemplo:** CPE(config-sla-monitor-pathEcho)# tos 240	(Opcional) Configura o Type of Service dos pacotes enviados pela operação. **Parâmetros:** value: valor do ToS O exemplo configura os pacotes com ToS 240

Operação DNS Query

Esta operação mede o tempo de resolução de um nome. É necessário configurar o servidor DNS a ser usado, assim como o nome a ser resolvido.

Tabela 125: Configuração de IP SLA DNS Query

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 6	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# type dns target-addr target name-server server **Exemplo:** CPE(config-sla-monitor)# type dns target-addr www.google.com name-server 8.8.8.8	Configura a operação do monitor para ser do tipo DNS Client. **Parâmetros:** target: nome a ser resolvido server: endereço IP do servidor DNS a ser usado. O exemplo configura a operação para ser do tipo DNS Query, resolvendo o nome www.google.com através do servidor dns 8.8.8.8
5	CPE(config-sla-monitor-dns)# description text **Exemplo:** CPE(config-sla-monitor-dns)# description dns Google	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição “dns google”
	CPE(config-sla-monitor-dns)# frequency secs **Exemplo:** CPE(config-sla-monitor-dns)# frequency 3600	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação dhcp do monitor para ser repetida a cada 3600 segundos.
	CPE (config-sla-monitor-dns)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-dns)# hours-of-statistics-kept 240	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 240 horas.

Operação TCP Echo

Esta operação funciona de forma parecida com um Echo, com a importante diferença que este "ping" não para na camada de rede. Uma conexão TCP é utilizada para que a requisição seja enviada e respondida. É preciso configurar um endereço IP de destino. Opcionalmente, é possível definir a quantidade de dados payload do pacote TCP e também o campo Type of Service (ToS) no pacote IP.

Por estar sendo utilizado um protocolo de transporte, diferentemente de um simples Echo (ou ping), **é necessário que o destino esteja configurado TCP Echo Responder.**

Tabela 126: Configuração de IP SLA TCP Echo

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 7	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# typetcpecho dest-addr destination **Exemplo:** CPE(config-sla-monitor)# typetcpecho dest-addr 192.168.11.1	Configura a operação do monitor para ser do tipo TCP Echo. **Parâmetros:** destination: endereço IP de destino O exemplo configura a operação para ser do tipo tcp echo com destino 192.168.11.1.
5	CPE(config-sla-monitor-tcpEcho)# description text **Exemplo:** CPE(config-sla-monitor-tcpEcho)# description tcpecho no gateway	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição "tcpecho no gateway"
	CPE(config-sla-monitor-tcpEcho)# frequency secs **Exemplo:** CPE(config-sla-monitor-tcpEcho)# frequency 90	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação do monitor para ser repetida a cada 90 segundos.

	CPE (config-sla-monitor-tcpEcho)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-tcpEcho)# hours-of-statistics-kept 3	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 3 horas.
	CPE (config-sla-monitor-tcpEcho)# timeout ms **Exemplo:** CPE(config-sla-monitor-tcpEcho)# timeout 5000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 5000 milissegundos (5 segundos).
	CPE (config-sla-monitor-tcpEcho)# size size **Exemplo:** CPE(config-sla-monitor-tcpEcho)# size 200	(Opcional) Configura o tamanho dos pacotes enviados pela operação. **Parâmetros:** size: tamanho do pacote em bytes O exemplo configura as operações com pacotes de 200 bytes.
	CPE (config-sla-monitor-tcpEcho)#tos value **Exemplo:** CPE(config-sla-monitor-tcpEcho)# tos 26	(Opcional) Configura o Type of Service dos pacotes enviados pela operação. **Parâmetros:** value: valor do ToS O exemplo configura os pacotes com ToS 26

Operação UDP Echo

Esta operação funciona de forma parecida com um Echo, com a importante diferença que este "ping" não para na camada de rede. É utilizado o protocolo de transporte UDP neste caso. É preciso configurar um endereço IP de destino. Opcionalmente, é possível definir a quantidade de dados payload do datagrama UDP e também o campo Type of Service (ToS) no pacote IP.

Por estar sendo utilizado um protocolo de transporte, diferentemente de um simples Echo (ou ping), **é necessário que o destino esteja configurado UDP Echo Responder.**

Tabela 127: Configuração de IP SLA UDP Echo

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 8	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# typeudpecho dest-addr destination **Exemplo:** CPE(config-sla-monitor)# type udpecho dest-addr 192.168.11.1	Configura a operação do monitor para ser do tipo UDP Echo. **Parâmetros:** destination: endereço IP de destino O exemplo configura a operação para ser do tipo udp echo com destino 192.168.11.1.
5	CPE(config-sla-monitor-udpEcho)# description text **Exemplo:** CPE(config-sla-monitor-udpEcho)# description udpecho no gateway	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição "udpecho no gateway"
	CPE(config-sla-monitor-udpEcho)# frequency secs **Exemplo:** CPE(config-sla-monitor-udpEcho)# frequency 180	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação do monitor para ser repetida a cada 180 segundos.

	CPE (config-sla-monitor-udpEcho)# hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-udpEcho)# hours-of-statistics-kept 36	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 36 horas.
	CPE (config-sla-monitor-udpEcho)# timeout ms **Exemplo:** CPE(config-sla-monitor-udpEcho)# timeout 2000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 2000 milissegundos (2 segundos).
	CPE (config-sla-monitor-udpEcho)# size size **Exemplo:** CPE(config-sla-monitor-udpEcho)# size 300	(Opcional) Configura o tamanho dos pacotes enviados pela operação. **Parâmetros:** size: tamanho do pacote em bytes O exemplo configura as operações com pacotes de 300 bytes.
	CPE (config-sla-monitor-udpEcho)#tos value **Exemplo:** CPE(config-sla-monitor-udpEcho)# tos 26	(Opcional) Configura o Type of Service dos pacotes enviados pela operação. **Parâmetros:** value: valor do ToS O exemplo configura os pacotes com ToS 26

Operação TWAMP

Uma operação Echo (ping) mede o tempo de ida e volta do pacote (RTT). Não se separa o tempo de ida do de volta. Se ocorre um problema apenas no caminho de ida e seu tempo aumenta, isso não é especificamente detectado pelo Echo, ele apenas irá dizer que o RTT aumentou. Com o TWAMP, as medidas de ida e de volta são feitas de forma independentes através de rajadas de pacotes UDP.

Chamamos de TWAMP-Client quem inicia a operação (quem configura o monitor) e TWAMP-Server o destino da operação (veja configuração mais adiante). O Client abre uma conexão TCP com o server e negocia o teste. Deste ponto em diante, ambos lançam rajadas de pacotes UDP em direção ao outro, utilizando marcas de numeração e tempo, o protocolo determina perdas, atraso e jitter unidirecionais nos dois caminhos (ida e volta).

Tabela 128: Configuração de IP SLA TWAMP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor number **Exemplo:** CPE(config)# ip sla monitor 9	Cria o monitor number e acessa o modo de configuração do monitor IP SLA.
4	CPE(config-sla-monitor)# type twamp destination **Exemplo:** CPE(config-sla-monitor)# type twamp dest-addr 192.168.11.1	Configura a operação do monitor para ser do tipo TWAMP. **Parâmetros:** destination: endereço IP do TWAMP-Server O exemplo configura a operação para ser do tipo TWAMP com destino 192.168.11.1.
	CPE(config-sla-monitor-twamp)#description text **Exemplo:** CPE(config-sla-monitor-twamp)#description Teste TWAMP Router Voz Operadora X	(Opcional) Configura uma descrição para o monitor. **Parâmetros:** text: texto que descreve a operação O exemplo configura a monitor com a descrição “Teste TWAMP Router Voz Operadora X”
	CPE(config-sla-monitor-twamp)#codec { g.711 | g.729 }	(Opcional) Habilita o cálculo de qualidade de ligação usando o codec selecionado. Não esquecer de ajudar o tamanho do pacote e o intervalo correto para o seu cenário.
	CPE(config-sla-monitor-twamp)#dscp dscp **Exemplo:** CPE(config-sla-monitor-twamp)#dscp 13	(Opcional) Configura o IP DSCP das rajadas de pacotes UDP enviados pelo Client e pelo Server. **Parâmetros:** dscp: valor do IP DSCP O exemplo configura os pacotes com DSCP 13

	CPE(config-sla-monitor-twamp)#frequency secs **Exemplo:** CPE(config-sla-monitor-twamp)#frequency 180	(Opcional) Configura a frequência das operações do monitor. **Parâmetros:** secs: frequência em segundos. O exemplo configura a operação do monitor para ser repetida a cada 180 segundos. Este é o intervalo entre cada rajada.
	CPE(config-sla-monitor-twamp)#hours-of-statistics-kept hrs **Exemplo:** CPE(config-sla-monitor-twamp)#hours-of-statistics-kept 24	(Opcional) Configura a longevidade das estatísticas coletadas pelas operações do monitor. **Parâmetros:** hrs: tempo em horas O exemplo configura o monitor para manter os resultados das últimas 24 horas.
	CPE(config-sla-monitor-twamp)#interval ms **Exemplo:** CPE(config-sla-monitor-twamp)#interval 50	(Opcional) Configura o intervalo entre os pacotes da rajada de cada teste, par aos dois lados. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as rajadas com intervalo de 50ms entre os pacotes
	CPE(config-sla-monitor-twamp)#packet-count pkts **Exemplo:** CPE(config-sla-monitor-twamp)#packet-count 50	(Opcional) Configura o número de pacotes em cada rajada. **Parâmetros:** pkts: número de pacotes O exemplo configura as rajadas com 50 pacotes. Quanto maior este número, maior a amostra. Deve-se cuidar para o instrumento de medida (TWAMP) não pertubar quem é medido (a REDE) e levantar estatísticas incorretas.
	CPE(config-sla-monitor-twamp)#receiver-port port **Exemplo:** CPE(config-sla-monitor-twamp)#receiver-port 50001	(Opcional) Configura a porta que o Client e o Server recebem seus pacotes da rajada. **Parâmetros:** port: número da porta UDP que recebe os pacotes da rajada. De ambos os lados. O exemplo configura a porta para 50001/UDP

	CPE(config-sla-monitor-twamp)#sender-port port **Exemplo:** CPE(config-sla-monitor-twamp)#sender-port 50002	(Opcional) Configura a porta que o Client e o Server enviam seus pacotes da rajada. **Parâmetros:** port: número da porta UDP que envia os pacotes da rajada. De ambos os lados. O exemplo configura a porta para 50002/UDP
	CPE(config-sla-monitor-twamp)#size bytes **Exemplo:** CPE(config-sla-monitor-twamp)#size 120	(Opcional) Configura o tamanho de cada pacote da rajada UDP. **Parâmetros:** bytes: tamanho do payload UDP em bytes **Observação:** o tamanho do pacote real pode resultar maior que esperado pois o protocolo precisa carregar algumas informações nesses pacotes. Se o tamanho configurado foi menor que o necessário para o cenário, o tamanho do pacote na rede pode ser maior que este configurado. Valores acima de 14 bytes não devem sofrer alteração. O exemplo configura para que cada pacote da rajada tenha 120 bytes de payload. Sem contar cabeçalhos de transporte, rede e enlace.
	CPE(config-sla-monitor-twamp)#start-delay ms **Exemplo:** CPE(config-sla-monitor-twamp)#start-delay 100	(Opcional) Configura um atraso entre a negociação do teste este Client e Server e o início das rajadas. **Parâmetros:** ms: tempo em milissegundos O exemplo configura a operação para começar 100ms depois da negociação entre o Client e Server.
	CPE(config-sla-monitor-twamp)#timeout ms **Exemplo:** CPE(config-sla-monitor-twamp)#timeout 2000	(Opcional) Configura o timeout de cada operação. É o tempo que cada operação pode demorar antes de ser considerada como falha. **Parâmetros:** ms: tempo em milissegundos O exemplo configura as operações com timeout de 2000 milissegundos (2 segundos).

4.12.2.2. Agendamento de Monitores

Após a configuração de um monitor, é necessário que se agende a sua execução para que ele possa coletar estatísticas. Este agendamento consiste em configurar horário de início, tempo de duração e recorrência. Estas configurações precisam ser feitas antes do início da execução do monitor. Além disso, existem ainda os comandos de reinício e parada forçados.

Horário de Início

O agendamento do horário de início é mostrado na tabela abaixo. Existem 4 modos: início pendente (não será iniciado), agora (início imediato), hh:mm (horário definido) e após (a execução inicia um certo número de segundos após a entrada do comando). Não existe configuração padrão e este comando necessita ser executado em um modo diferente de pendente para que a operação do monitor seja iniciada.

Tabela 129: Configuração de Horário de Início do Monitor IP SLA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor schedule number start-time { pending | now | hh:mm | after { secs } } **Exemplo:** CPE(config)# ip sla monitor schedule 2 start-time after 600	Configura o monitor para que inicie suas operações em um determinado horário. **Parâmetros:** number: número do monitor pending: deixa o horário de início pendente now: inicia imediatamente hh:mm: inicia no horário hh:mm secs: inicia em secs segundos O exemplo configura o monitor número 2 para iniciar em 600 segundos.

Tempo de Duração

A configuração de tempo de duração define por quanto tempo um monitor executará suas operações após seu início. Esta configuração pode ser de dois modos: para sempre ou um tempo de execução definido em segundos. A configuração padrão é para sempre.

Tabela 130: Configuração do Tempo de Duração da Operação do Monitor IP SLA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor schedule number life { forever | seconds } **Exemplo:** CPE(config)# ip sla monitor schedule 2 life 500	Configura o tempo de duração das operações do monitor. **Parâmetros:** number: número do monitor forever: deixa o horário de início pendente seconds: inicia imediatamente O exemplo configura o monitor número 2 para que termine 500 segundos após o início.

Recorrência

Caso o monitor seja configurado com um horário de início do tipo HH:MM e tempo de duração menor que 24 horas, é possível configurar recorrência. Com esta configuração, o monitor é executado todos os dias no horário de início especificado, com o tempo de duração definido. A configuração padrão é não recorrente.

Tabela 131: Configuração de Recorrência do Monitor IP SLA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor schedule number recurring **Exemplo:** CPE(config)# ip sla monitor schedule 2 recurring	Configura o tempo de duração das operações do monitor. **Parâmetros:** number: número do monitor O exemplo configura o monitor número 2 para que inicie suas operações todos os dias. **Atenção:** esta configuração deve ser utilizada sempre em conjunto com a configuração de horário de início com hora marcada (hh:mm).

Parada Forçada

Este comando serve para forçar a parada de execução de um monitor ativo. É necessário quando se deseja modificar configurações do monitor e ele esteja no estado ativo (executando).

Tabela 132: Parada das Operações de um Monitor IP SLA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor schedule number stop-now **Exemplo:** CPE(config)# ip sla monitor schedule 2 stop-now	Finaliza as operações de um monitor. **Parâmetros:** number: número do monitor O exemplo para as operações do monitor número 2.

Reinício

Este comando serve para forçar o reinício da execução de um monitor ativo. Útil após uma parada forçada.

Tabela 133: Reinício das Operações de um Monitor IP SLA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor restart number **Exemplo:** CPE(config)# ip sla monitor restart 2	Reinicia um monitor ativo. **Parâmetros:** number: número do monitor O exemplo reinicia as operações do monitor número 2.

TCP Echo e UDP Echo Responders

Os comandos para habilitar os serviços de TCP e UDP Echo Responders são mostrados abaixo. A primeira tabela mostra como habilitar o serviço para TCP e a segunda, UDP.

Tabela 134: Habilitando TCP Echo Responder

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# service tcp-echo-responder	Habilita resposta de TCP Echo.

Tabela 135: Habilitando UDP Echo Responder

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# service udp-echo-responder	Habilita resposta de TCP Echo.

Twamp Server

Para que uma outra entidade possa realizar testes TWAMP contra o CPE, é necessário ligar o TWAMP Server.

Tabela 136: Habilitando o TWAMP Server

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# twamp server [vrf vrf]	Habilita o TWAMP Server.

4.12.3. Visualização de Estado e Configurações

Para que se possa acompanhar o estado da aplicação IP SLA Monitor, as configurações dos monitores e as configurações de agendamento de cada monitor, existem três comandos.

4.12.3.1. Estado do IP SLA Monitor

O estado do IP SLA Monitor mostra o número de monitores (entries) configurados e o estado de cada um. Entradas ativas estão em execução. Entradas pendentes estão agendadas para execução, mas ainda não iniciaram, ou ainda foram configuradas como pendentes. Por último, entradas inativas já terminaram sua execução ou não foram agendadas.

```
CPE>show ip sla monitor application
      IP Service Level Agreement Monitor
Number of Entries configured
: 2
Number of active Entries
: 1
Number of pending Entries
: 0
Number of inactive Entries
: 1

      Supported Operation Types
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: pathEcho
Type of Operation to Perform: tcpEcho
Type of Operation to Perform: udpEcho
Type of Operation to Perform: TWAMP
```

4.12.3.2. Configurações do IP SLA Monitor

Para cada monitor configurado são mostradas todas suas configurações, exceto agendamento. O parâmetro opcional especifica que se deseja apenas visualizar a configuração de um monitor específico, especificado por um número.

```
CPE>show ip sla monitor configuration  [ número do monitor ]
Entry number: 2
    Type of operation to perform: echo
    Target address: 192.168.10.100
    Source address: not configured
    Operation timeout (milliseconds): 5000
    Type Of Service: 0
    Operation frequency (seconds): 60
    Packet size (bytes): 56
    Packet TTL: 255
    Number of statistic hours kept: 6
Entry number: 3
    Type of operation to perform: ftp
    Description:
    Destination: ftp://ftp.br.debian.org/debian/README.html
    Operation timeout (milliseconds): 5000
    Operation frequency (seconds): 60
    Number of statistic hours kept: 6
```

4.12.3.3. Agendamentos do IP SLA Monitor

Para cada monitor configurado, é mostrado seu agendamento. O parâmetro opcional especifica que se deseja apenas visualizar a configuração de um monitor específico, especificado por um número.

```
CPE>show ip sla monitor schedule [ número do monitor ]
Entry number: 2 - echo
    Status: inactive
    Operation life: 6000 seconds
    Recurring: every day at 09:45
    Start time: 09:45
Entry number: 3 - ftp
    Status: active
    Operation life: forever
Recurring: no
    Start time: immediate
```

4.12.3.4. Obtenção de Resultados e Estatísticas

Conforme as configurações de agendamento de um monitor, ele iniciará suas operações. Após um certo tempo, estarão disponíveis as informações coletadas por ele. A obtenção destes resultados deve ser feita através do comando show ip sla monitor statistics. Este comando pode mostrar os resultados de todos monitores (uso do comando sem parâmetros opcionais) ou de apenas um dos monitores.

Pode-se especificar ainda, o tamanho da janela de amostragem para a obtenção de estatísticas e resultados. Este valor indica quantos minutos de operações devem ser agrupados para o cálculo das estatísticas. Por exemplo, para uma operação com frequência de 30 segundos, um tamanho de janela de 5 minutos, reunirá em um mesmo grupo 10 operações. O valor padrão da janela de amostragem, caso não especificado, é de 5 minutos. O exemplo abaixo mostra a obtenção de estatísticas e resultados para o monitor 1 com janela de 10 minutos.

Comando:

show ip sla monitor statistics [número do monitor | window-size { minutos }{ monitor }]

Exemplo:

CPE>**show ip sla monitor statistics window-size 101**
Entry number: 1
Type of operation: echo
Description: ping gateway
Statistics kept up to the last 72 hours of operation
Operation started on Fri Aug 26 13:30:15 2011
At 13:35:15
RTT Moving Average: 1.368ms
Packet RTT Variation: 1.1143ms²2
Packet Loss: 0% (0 packets)
At 13:45:15
RTT Moving Average: 0.8808ms
Packet RTT Variation: 0.0004907ms²2
Packet Loss: 0% (0 packets)
.....

Observação: O monitor do tipo TWAMP ignora o parâmetro window-size. As estatísticas aparecerão para cada operação realizada.

4.12.4. Reações e Limiares de Operações SLA

4.12.4.1. Configuração dos Limiares e Reações

As estatísticas coletadas pelas operações configuradas nas últimas seções não servem apenas para visualização. É possível utilizar estes dados para se configurar limiares independentes para cada monitor SLA. Então, conforme os dados coletados e as configurações dos limiares pode-se gerar uma Trap, disparar outro monitor, ou não fazer nada.

Todo limiar possui em valor superior e um inferior. O valor superior indica um valor que, igual ou acima, a reação é ativada e o SLA é considerado com problemas (ou down). O valor inferior indica um valor que, igual ou abaixo, a reação é desativada e o SLA é considerado ok (ou up).

Além disso, todo limiar possui um tipo. Os tipos podem ser:

- Average (média): quando a média dos últimos N valores obtidos pela operação cruza um valor do limiar.
- Consecutive (ocorrências consecutivas): quando todos os últimos N valores obtidos pela operação cruzam um valor do limiar
- Immediate (imediato): quando o último valor obtido pela operação cruza um valor do limiar.
- Never (nunca): nunca reage.
- xofy (X de Y): quando X dos últimos Y valores obtidos pela operação cruzam um valor do limiar.

Para que se possa entender melhor, vamos fazer um exemplo antes de configurar. Suponha que o monitor SLA 123 coletou dados, e os últimos foram:

1 3 2 1 2 3 4 2 5 3 6 6 1 2 6 2 1

Suponha que os valores dos limiares são:

- 4 para o limiar superior
- 2 para o limiar inferior

Para configuração xofy com X = 3 e Y = 5, temos uma janela de 5 (Y) valoes, buscamos 3 (X) valores acima do limiar superior para ativar a reação e 3 calores abaixo do valor inferior para desativarmos a reação. Com isso, teríamos num primeiro instante

T = 1

{1,3,2,1,2}; Todos os valores abaixo do limiar superior, não reage

T = 2

{3,2,1,2,3}; Todos os valores abaixo do limiar superior, não reage

T = 3

{2,1,2,3,4}; Apenas 1 valor acima do limiar superior, não reage

T = 4

{1,2,3,4,2}; Apenas 1 valor acima do limiar superior, não reage

T = 5

{2,3,4,2,5}; Apenas 2 valores acima do limiar superior, não reage

T = 6

{3,4,2,5,3}; Apenas 2 valores acima do limiar superior, não reage

T = 7

{4,2,5,3,6}; 3 valores acima do limiar superior, reage

T = 8

{2,5,3,6,6}; Apenas 1 valor abaixo do limiar inferior, continua sinalizando reação

T = 9

{5,3,6,6,1}; Apenas 1 valor abaixo do limiar inferior, continua sinalizando reação

T = 10

{3,6,6,1,2}; Apenas 2 valores abaixo do limiar inferior, continua sinalizando reação

T = 11

{6,6,1,2,6}; Apenas 2 valores abaixo do limiar inferior, continua sinalizando reação

T = 11

{6,1,2,6,2}; 3 valores abaixo do limiar inferior, acaba a sinalização e volta ao estado "ok"

T = 12

{1,2,6,2,1}; 3 valores abaixo do limiar superior, não reage

Para configurar este mecanismo, utilize os comandos abaixo:

Tabela 137: Habilitando SLA Reaction

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#ip sla monitor reaction-configuration monitor react { jitter | rtt | timeout } action-type { none, trapandtrigger, traponly, triggeronly } threshold-type { average *n* / consecutive *n* | immediate | never | xofy *x y* } threshold-value { *lower higher* } Exemplo: CPE(config)#ip sla monitor reaction-configuration 1 react rtt action-type trapandtrigger threshold-type xofy 3 5 threshold-value 20 40	Habilita SLA Reaction. **Monitor:** número do monitor SLA que se deseja adicionar configurações de reação. **React:** jitter, rtt ou timeout. Escolha a variável que você deseja monitorar. Note que nem todos tipos de monitores coletam todas as variáveis. **Action-Type:** escolha se não é para fazer nada, enviar trap SNMP, apenas gatilho (veja seção de abaixo) ou ambas. Escolha “none” caso apenas queira usar apenas Tracks. **Threshold value:** escolha os limiares inferior e superior. Os valores padrão para caso se deixe as configurações em branco são: threshold-type Average 5 action-type Trapandtrigger threshold-value 15 500 O exemplo configura o equipamento para trapandtrigger, ou seja, enviar traps SNMP e disparar outra operação SLA (caso um trigger esteja configurado) caso o valor de rtt supere 40 considerando o mecanismo 3 de 5.

4.12.4.2. Gatilho - Reagir com a Ativação de um Outro Monitor

Caso o tipo de ação action-type, configurada no item anterior inclua “trigger” podemos configurar para que um novo monitor sla seja disparado. Evidentemente este monitor deve estar previamente configurado.

Para fazer isso, use os comandos da tabela abaixo.

Tabela 138: Habilitando SLA Trigger

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ip sla monitor reaction-trigger *reaction-monitor target-monitor* Exemplo: CPE(config)# ip sla monitor reaction-trigger 1 2	Habilita SLA Trigger. **Reaction-monitor:** número do monitor SLA que se deseja adicionar configurações de trigger. **Target-monitor:** número do monitor SLA que deve ser disparado caso o monitor acima encontre problemas. O exemplo configura o equipamento para que se for detectado algum problema no monitor 1, o monitor 2 seja iniciado.

4.13. Tracks

Tracks são muito úteis para realizar tarefas de monitorar rotas, interfaces ou operações SLA e tomar ações caso os parâmetros monitorados saiam dos limiares especificados. Cada track é identificada por um número, que pode ser especificado entre 1 e 1000.

Depois de configurados, os Tracks podem ser utilizados em diversos pontos do roteador. Por exemplo, para uma rota estática depender de um Track, usa-se a opção de track no comando que insere a rota:

- CPE(config)#ip route vrf RED 40.30.20.0/24 ethernet 1 128 **track 5**

ou ainda, para a instalação de um name-server depender de um track, podemos fazer:

- CPE(config)#ip name-server 8.8.8.8 **track 7**

Note o potencial de configuração desta ferramenta: podemos configurar uma operação SLA ICMP (um simples ping) para um destino que nos interessa, configuramos também um SLA Threshold para esta operação, dizendo que pings acima de 30ms devem ser interpretados como problema. Em cima disso, fazemos um track monitorando a operação SLA. Toda vez que os pings da operação estiverem do limiar de 30ms, o track indica a mudança para a configuração que depende dele. Ou seja, se os pings com a rota atual superarem 30ms, podemos instalar uma nova rota por outro caminho, mesmo que a interface continue conectada e “up”. Muitas outras coisas muito interessantes podem ser feitas.

Ação deste Threshold (configurado no SLA Reaction) pode ser “none”.

4.13.1. Tracking de Rotas IP

Neste módulo temos duas opções. Verificar se um destino é simplesmente alcançável através da tabela de rota ou verificar se ela é alcançável e com uma restrição de métrica. Vale ressaltar que isso não garante que o destino seja alcançável, apenas garante que existe a rota. Para ver se o destino é alcançável utilize Tracking de operações SLA, explicados mais adiante.

4.13.1.1. Se é Alcançável

Este tipo de track serve para monitorar se um determinado destino é alcançável pela tabela de rotas. Por exemplo, podemos configurar um Track para monitorar se é possível alcançar o destino 1.2.3.4/32 através da tabela de rotas. Para fazer isso, seguem os comandos abaixo:

Tabela 139: Tracking de Rotas IP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track 1 ip route 1.2.3.4/32 reachability	Entra no modo de configuração da track 1 monitorando se o endereço 1.2.3.4/32 é alcançável.
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.13.1.2. Usando Limiares de Métrica

Este tipo de track serve para monitorar se um determinado destino é alcançável com limite máximo de métrica. Por exemplo, podemos verificar se o destino 1.2.3.4/32é alcançável com métrica abaixo de 120.

Para fazer isso, seguem os comandos abaixo:

Tabela 140: Tracking de Rotas IP por Métrica

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track track ip route 1.2.3.4/32 metric-threshold Exemplo: CPE(config)# track 1 ip route 1.2.3.4/32 metric-threshold	Entra no modo de configuração da track *track* monitorando se o endereço 1.2.3.4/32 é alcançável e com limiares de métrica. **track:** identificador da track. Entre 1 e 1000.
4	CPE(config-track)# threshold metric up *up* down *down* Exemplo: CPE(config-track)# threshold metric up 10 down 20	Configura os valores de métrica para que se considere o track up ou down. **up:** considera-se o track como up com a métrica da rota com valor de até *up.* **down:** considera-se o track como down com a métrica da rota com valor de *down* em diante. No exemplo o Track irá para UP toda vez que a métrica alcançar 10 (no sentido decrescente) e ira para DOWN toda vez que a métrica passar de 20 (no sentido crescente).
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.13.2. Tracking de Operações SLA

A função de Tracking funciona junto com o IP SLA neste caso. No caso “Se a Operação Alcança o Destino” podemos monitorar se a operação SLA está sendo bem sucedida ou retornando erro. Já no caso “Pelo Estado do SLA-Treshold” podemos monitorar se a operação SLA está funcionando e dentro dos parâmetros de tolerância especificados no SLA-Threshold.

4.13.2.1. Se a Operação Alcança o Destino

Neste caso o Track vai monitorar se a operação SLA está sendo bem sucedida ou não. Um ICMP Echo que não se recebe um ICMP Reply é considerado uma operação mal sucedida. Um valor extremamente alto de RTT ainda é considerado uma operação bem sucedida. Para configurar, use os comandos abaixo:

Tabela 141: Tracking de IP SLA Reachability

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track track ip sla sla reachability Exemplo: CPE(config)# track 1 ip sla 33 reachability	Entra no modo de configuração da track *track* monitorando a operação SLA *sla* **track:** identificador da track. Entre 1 e 1000. **sla:** identificador da operação SLA previamente configurada.
4	CPE(config-track)#default-state { up | down }	Configura o valor padrão e inicial da track. Valor padrão é usado caso a operação SLA não esteja sendo executada no momento.
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.13.2.2. Pelo Estado do SLA-Threshold

Tabela 142: Tracking de IP SLA Reachability

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track *track* ip sla sla state Exemplo: CPE(config)# track 1 ip sla 5 state	Entra no modo de configuração da track *track* monitorando o SLA-Threshold da operação SLA *sla*. **track:** identificador da track. Entre 1 e 1000. **sla:** identificador da operação SLA e se respectivo SLA-Threshold previamente configurados.
4	CPE(config-track)#default-state { up | down }	Configura o valor padrão e inicial da track. Valor padrão é usado caso a operação SLA não esteja sendo executada no momento.
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.13.3. Tracking de Interfaces

4.13.3.1. Protocolo de Linha

Este track é bastante simples: monitora se o LINE-PROTOCOL da interface está up. Em termos gerais, se tem cabo conectado corretamente. Para configurar, siga os passos abaixo:

Tabela 143: Tracking de Interface Line-Protocol

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track *track* interface interface line-protocol Exemplo: CPE(config)# track 1 interface ethernet1 line-protocol	Entra no modo de configuração da track *track* monitorando o line-protocol da interface *interface* **track:** identificador da track. Entre 1 e 1000. **intreface:** a interface que se deseja monitorar
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.13.3.2. Roteamento IP

Este track monitora se a interface roteia pacotes IP/IPv6. Por exemplo, se a interface é movida para um bridge-group, ela deixa de rotear pacotes. Para configurar, siga os passos abaixo:

Tabela 144: Tracking de Interface Routing

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# track *track* interface *interface* ip routing Exemplo: CPE(config)# track 1 interface ethernet1 ip routing	Entra no modo de configuração da track *track* monitorando se a interface *interface* é capaz de rotear pacotes. **track:** identificador da track. Entre 1 e 1000. **intreface:** a interface que se deseja monitorar
	CPE(config-track)#delay { down | up } tempo	(Opcional) Configura um atraso para o track mudar de estado. **down:** configura atraso para mudar de up para down **up:** configura atraso para mudar de down para up **tempo:** tempo em segundos
	CPE(config-track)#description *texto*	(Opcional) Adiciona uma descrição para o track.

4.14. Internet Protocol Security (IPsec)

(recurso habilitado por licença)

IPsec é um conjunto de protocolos que têm como objetivo autenticar e criptografar uma comunicação. Ele pode ser utilizado para proteger os fluxos entre dois hosts (host-to-host), duas redes (net-to-net) ou entre um host e uma rede (host-to-network).

4.14.1. Considerações Iniciais

O IPsec opera na camada de rede, imediatamente acima do IP. Isso o diferencia fundamentalmente de outros protocolos de segurança como o SSL, TLS ou SSH. Enquanto estes últimos precisam ser configurados em camadas superiores, o IPsec é transparente para qualquer comunicação que utilize IP.

Os principais conceitos que devem estar claros neste ponto são:

- Integridade: garantia de que os dados recebidos são idênticos aos enviados.
- Confidencialidade: garantia de que os dados enviados podem ser lidos apenas pelo destinatário.
- Autenticidade: garantia da identidade do emissor.

AH, ESP e ISAKMP/IKE são os protocolos utilizados pelo IPsec para cumprir suas funções de integridade, confidencialidade e autenticidade. O primeiro protocolo fornece os serviços de autenticação e integridade. O ESP fornece, dependendo do modo que atua, autenticação, integridade e confidencialidade. Os últimos são protocolos que possibilitam o estabelecimento/negociação das conexões seguras. Veja a tabela abaixo para comparar as funcionalidades do AH e do ESP. Estes dois protocolos podem ser utilizados ao mesmo tempo caso se queira.

Tabela 145. Serviços dos Protocolos do IPsec.

Protocolo/Serviço	Integridade	Autenticidade	Confidencialidade
ESP Modo Transporte	Não	Não	Sim
ESP Modo Túnel	Sim	Sim	Sim
AH	Sim	Sim	Não

O IPsec possui dois modos básicos de operação: transporte e túnel. No modo de transporte o pacote IP original tem sua carga criptografada caso seja utilizado o serviço de confidencialidade (ESP transporte). Além disso, pode ser inserido o AH na frente do pacote IP para fornecer os serviços de integridade e autenticidade.

Já no modo túnel, o pacote IP original é usado como carga de um novo pacote ESP (túnel), e os serviços de integridade, autenticidade e confidencialidade são fornecidos. Como os três serviços já são fornecidos pelo protocolo ESP no modo túnel, não faz sentido utilizar o protocolo AH em configurações de IPsec no modo túnel.

Cada modo do IPsec usa diferentes combinações de ESP e AH. No total, são possíveis três combinações no modo transporte e duas no modo túnel. Uma combinação não faz sentido (como explicado no parágrafo anterior) e outra é insegura. Observe na tabela abaixo todas as possíveis combinações:

Tabela 146. Modos IPsec.

Modo IPsec	ESP	AH	Integridade	Autenticidade	Confidencialidade
(1) Transporte	-	Sim	Sim (AH)	Sim (AH)	Não
(2) Transporte	Transporte	Sim	Sim (AH)	Sim (AH)	Sim (ESP)
(3) Transporte	Transporte	-	Não	Não	Sim (ESP)
(4) Túnel	Túnel	Sim	Sim (AH e ESP)	Sim (AH e ESP)	Sim (ESP)
(5) Túnel	Túnel	Não	Sim (ESP)	Sim (ESP)	Sim (ESP)

IMPORTANTE: o modo (3) é inseguro e não deve ser utilizado. O modo (4) não é utilizado pois o modo (5) fornece o mesmo serviço de forma mais simples (sem AH). Use apenas (1), (2) e (5), dependendo dos objetivos.

Portanto, na prática, acima se resume em:

Tabela 147. Modos IPsec na Prática.

Modo IPsec	ESP	AH	Integridade	Autenticidade	Confidencialidade
(1) Transporte	-	Sim	Sim (AH)	Sim (AH)	Não
(2) Transporte	Transporte	Sim	Sim (AH)	Sim (AH)	Sim (ESP)
(5) Túnel	Túnel	Não	Sim (ESP)	Sim (ESP)	Sim (ESP)

O modo (1) pode ser usado para estabelecer uma comunicação entre dois hosts com a garantia de que os pacotes foram de fato originados no outro host e que seu conteúdo não foi alterado.

O modo (2) adiciona ao modo (1) o serviço de confidencialidade: nenhuma entidade além dos dois hosts é capaz de ler a mensagem enviada.

O modo (5) é usado para estabelecer uma comunicação segura entre duas redes, com garantias de integridades, autenticidade e confidencialidade. Neste modo os pacotes podem passar sofrer NAT sem prejuízo.

De forma geral, recomenda-se o uso do modo (5) sempre que possível.

4.14.2. Mecanismos Suportados

Dependendo das características do equipamento, alguns destes mecanismos podem não estar disponíveis ou afetarem significativamente o desempenho da rede.

IPsec (RFC 2401 e RFC 2407)
OAKLEY (RFC 2412)
ISAKMP (RFC 2408)
IKE (RFC 2409)

Chaves RSA:

- Geração (360 a 4096 bits).
- Importação e exportação.

Certificados X.509v3:

- Geração (Autoridade Certificadora - PKI Offline)
- Importação/Exportação manual
- SCEP (Simple Certificate Enrollment Protocol) – Online PKI Enrollment
- CRL
- OCSP

AH (RFC 2402):

- MD5
- SHA

ESP (RFC 2406):

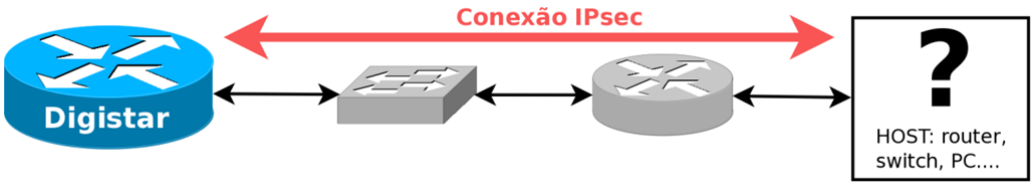
- DES
- 3DES
- NULL
- AES (128, 192 e 256 bits)

Diffie-Hellman:

- Group 2 (1024 bits)
- Group 5 (1536 bits)
- Group 14 (2048 bits)
- Group 15 (3072 bits)
- Group 16 (4096 bits)

4.14.3. Cenários de Uso

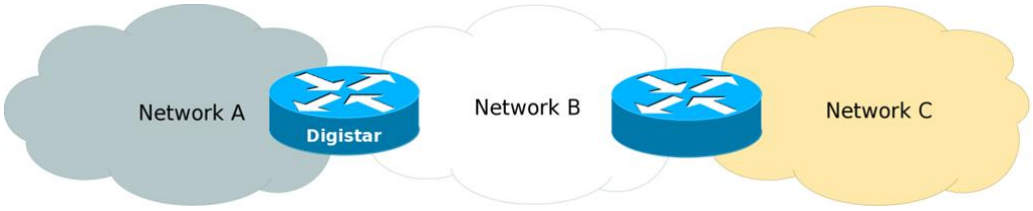
Existem três casos gerais de uso do IPsec: host-to-host, net-to-net e host-to-network (chamamos de VPN ou Roadwarrior). As configurações para cada caso são dadas na próxima seção.



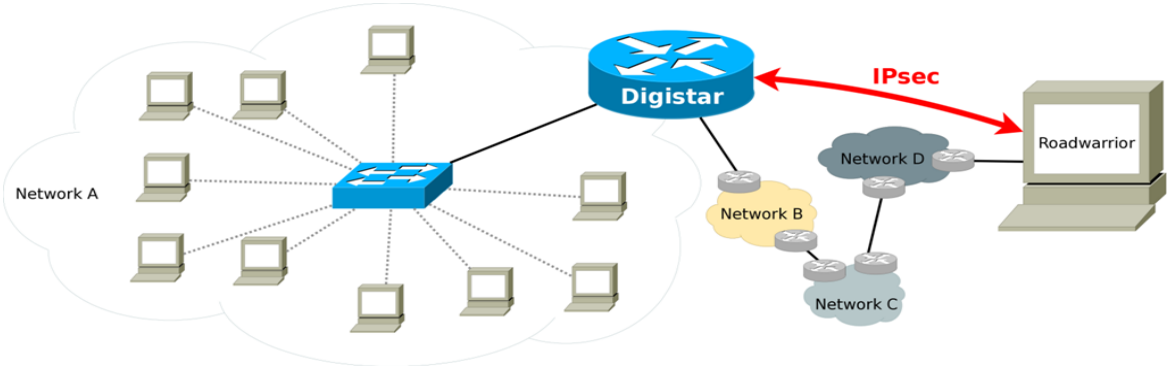
4.14.3.1. Host-to-Host

No caso de uso host-to-host apenas os pacotes IP com origem em um dos hosts e destino o outro host são protegidos. Qualquer outro pacote não é protegido (ex.: pacotes encaminhados). A conexão é feita entre o equipamento Digistar e um outro host qualquer (inclusive outro equipamento Digistar).

4.14.3.2. Net-to-Net



Conforme o exemplo da figura acima, no caso net-to-net, são protegidos todos os pacotes com origem na rede A, que passam pelo roteador Digistar e que tenham como destino a rede C. Da mesma forma, todos os pacotes com origem na rede C, que passam pelo outro roteador e que tenham como destino a rede A, também são protegidos. Para este cenário é necessário um equipamento roteador Digistar e algumoutro roteador compatível.



4.14.3.3. VPN

No caso VPN/Roadwarrior, conforme mostrado na figura acima, existe uma rede que o roteador Digistar dá acesso, sendo que esta rede possui diversos hosts interconectados por um switch. A idéia é fazer com que o host Roadwarrior, que não pertence ao enlace de A, faça parte da rede de A. Para os hosts do enlace A, o Roadwarrior está presente em sua rede de forma transparente. Além do mais, os pacotes entre Roadwarrior e Digistar devem trafegar pelas redes B, C e D com garantias de autenticidade, integridade e confidencialidade.

4.14.4. Configuração

A configuração de IPsec pode ser dividida em algumas etapas:

- Seleção do tráfego: utiliza-se uma access-list do tipo extended para selecionar o tráfego IPsec. Access-list de ação permit são usadas para isso. Por exemplo, caso se queira uma conexão segura apenas para pacotes TCP porta de origem 22 da rede X para a Y, utiliza-se a ACL na seguinte forma: access-list <N> permit tcp <X> eq 22 <Y>
- Conjuntos de Transformação: define a transformada da conexão. Nele configuram-se combinações dos algoritmos de criptografia (AES, DES, PFS...). Estes parâmetros influenciam a segurança da conexão.
- Políticas ISAKMP: define os parâmetros de transformada aceitos para a negociação da conexão.
- Crypto-Map: basicamente unifica todas as configurações acima em uma única entidade, além de definir o outro peer da conexão. Este é configurado na interface para habilitar IPsec.

Portanto, para configurar IPsec, primeiro deve-se configurar uma ACL para definir qual o tráfego que fará parte da conexão, depois um transform-set para definir os algoritmos de criptografia utilizados, então uma isakmp-policy para definir os parâmetros de negociação da conexão e por último um crypto-map, que referencia todos acima e ainda configura alguns parâmetros adicionais, como método de autenticação e peer.

É importante ressaltar que a configuração de IPsec deve ser feita em todos equipamentos que participem da conexão. Este manual cobre apenas como configurar o equipamento Digistar, com alguns exemplos de interoperabilidade com outros fabricantes bastante conhecidos.

4.14.4.1. Configurações Básicas

4.14.4.1.1. Pre-Shared Key

A forma mais básica de autenticação é PSK. Além dela, certificados são suportados, mas serão explicados mais adiante.

Tabela 148: Configuração de PSK

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# crypto isakmp key key { address address | hostname name } **Exemplo:** CPE (config)# crypto isakmp key teste123 address 192.168.11.1	Configura uma PSK para ser utilizada com um host. O exemplo configura para que o roteador utilize a PSK teste123 quando tentar estabelecer uma conexão segura com

4.14.4.1.2. Access-Lists

As ACLs selecionam o tráfego seguro. Precisam ser do tipo EXTENDED. Por exemplo, para definir que todo tráfego IP que deixa a rede 192.168.11.0/24 tendo como destino a rede 10.1.2.0/24 deve ser seguro, utiliza-se a access-list abaixo:

access-list 100 permit ip 192.168.11.0 0.0.0.255 10.1.2.0 0.0.0.255

Para mais informações, veja o capítulo deAccess Control Lists - ACLs

4.14.4.1.3. Transform Sets

Esta configuração define a transformada da conexão IPsec. A transformada é usada na proposta de conexão enviada ao peer.

Tabela 149: Configuração de Crypto Transform Set

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# crypto ipsec transform-set name [ah { md5-hmac | sha-hmac }] [comp-lzs] [esp-auth { md5-hmac | sha-hmac }] [esp-cipher { 3des | aes-128 | aes-192 | aes-256 | des | null }] [mode { transport | tunnel }] **Exemplo:** CPE (config)# crypto ipsec transform-set tset esp-auth md5-hmac esp-cipher 3des	(OPCIONAL) ah: algoritmo do protocolo AH (OPCIONAL) esp-auth: algoritmo de autenticação do protocolo ESP. (OPCIONAL) esp-cipher: algoritmo de cifragem do protocolo ESP. (OPCIONAL) mode: modo túnel (padrão) ou modo transporte. Observação: é necessário que se utilize pelo menos um dos três primeiros e que a configuração seja consistente. O exemplo configura um transform-set de nome tset para um túnel esp com autenticação md5 e cifragem 3des.

4.14.4.1.4. ISAKMP Policies

As políticas ISAKMP estão relacionadas com os parâmetros usados na negociação das conexões. Em geral, configura-se uma série de políticas, cada uma com uma prioridade e o roteador tentará negociar com o outro peer a de maior prioridade possível. A proposta do outro peer deve estar contida no conjunto de políticas configuradas para que a conexão seja aceita.

Tabela 150: Configuração de Crypto ISAKMP Policy

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# crypto isakmp policy num **Exemplo:** CPE(config)# crypto isakmp policy 1	Entra no diretório de configuração da política ISAKMP de prioridade num. Quanto menor o número maior a prioridade. O exemplo entra na política de prioridade máxima (1).
4	CPE(config-isakmp)# description TEXT	(OPCIONAL) Adiciona uma descrição para a política.
5	CPE(config-isakmp)# encryption { 3des | aes-128 | aes-192 | aes-256 } **Exemplo:** CPE(config-isakmp)# encryption 3des	Define a algoritmo de criptografia utilizado. O exemplo configura a política 1 para usar 3des.
5	CPE(config-isakmp)# group { 2 | 5 | 14 | 15 | 16 } **Exemplo:** CPE(config-isakmp)# group 2	Define o grupo Diffie-Hellman para PFS. 2 = 1024 bits 5 = 1536 bits 14 = 2048 bits 15 = 3072 bits 16 = 4096 bits O exemplo configura a política 1 para usar 1024 bits.
6	CPE(config-isakmp)# hash { md5 | sha } **Exemplo:** CPE(config-isakmp)# hash md5	Define o algoritmo de hash da política. O exemplo configura a política 1 para usar md5.

4.14.4.1.5. Crypto Map

O Crypto-Map é a peça chave na configuração de conexões IPsec. Esta entidade é instalada na interface que se deseja habilitar uma (ou mais) conexões seguras. Cada Crypto-Map possui um nome e pode ter diversas entradas (de 1 a 64). Pode-se, por exemplo, ter um Crypto-Map chamado EMPRESA, que possui duas instâncias (1 e 2), cada uma com parâmetros de configuração diferentes (transform-sets, ACLs, peers...).

Tabela 151: Configuração de Crypto ISAKMP Map

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# crypto map name num ipsec-isakmp **Exemplo:** CPE(config)# crypto map cmap 1 ipsec-isakmp	Entra no diretório de configuração do crypto map name de entrada num. O exemplo entra no mapa cmap de entrada 1.
4	CPE(config-crypto-map)#authentication { pre-share | certificate trustpoint }	Define o método de autenticação, pre-share (PSK) ou certificados (necessário um trustpoint configurado, ver na seção de certificados)
5	CPE(config-crypto-map)#connection { always | on-demand }	(OPCIONAL) Define como a conexão deve ser iniciada. Always: sempre ativa on-demand: negociada e iniciada sob demanda.
5	CPE(config-crypto-map)#description TEXT	(OPCIONAL) Adiciona uma descrição para a entrada no crypto-map.
6	CPE(config-crypto-map)#match ACL	Configura a ACL que selecionará os pacotes para esta entrada do crypto-map.
7	CPE(config-crypto-map)#set identity name	(OPCIONAL) Parâmetro usado apenas para autenticação por certificados (item 4). Define restrições sobre a identidade do outro peer.
8	CPE(config-crypto-map)#set ip-address { A.B.C.D | A.B.C.D/M | X:X::X:X | X:X::X:X/M | request } **Exemplo:** CPE(config-crypto-map)#set ip-address 2005::/64	(OPCIONAL) Parâmetro usado para requerir ou fornecer endereços IP para o peer. O exemplo configura para que o roteador Digistar peça um endereço IPv6 na faixa 2005::/64 para o peer.
9	CPE(config-crypto-map)#set peer { A.B.C.D | X:X::X:X }	Configura o endereço IP do peer.
10	CPE(config-crypto-map)#set pfs { group2 | group5 | group14 | group15 | group16 }	(OPCIONAL) Configura para usar PFS na proposta de parâmetros.
11	CPE(config-crypto-map)#set security-association idle-time seconds	(OPCIONAL) Configura o tempo que a conexão deve ficar inativa para que seja finalizada.

12	CPE(config-crypto-map)#set security-association lifetime seconds	(OPCIONAL) Configura o tempo que a conexão deve ser reiniciada (e os parâmetros renegociados).
13	CPE(config-crypto-map)#set transform-set name	Configura o transform-set a ser usado.
14	CPE(config-crypto-map)#version { ikev1 | ikev2 }	(OPCIONAL) Configura a versão do protocolo IKE a ser usado. **Observação:** para maior compatibilidade com equipamentos CISCO, utilize ikev1.

4.14.4.2. HOST-to-HOST

Para configurar uma conexão host-host, utiliza-se uma ACL com a palavra-chave host. Por exemplo, para uma conexão IP do host 192.168.11.1 para o host 192.168.11.2 utiliza-se a seguinte ACL:

access-list 150 permit ip host 192.168.11.1 host 192.168.11.2

É evidente que no outro peer é necessária uma configuração compatível. Caso for um roteador Digistar, pode-se utilizar a mesma ACL, entretanto, trocam-se os endereços IP de origem e destino:

access-list 150 permit ip host 192.168.11.2 host 192.168.11.1

4.14.4.3. NET-to-NET

Para uma conexão NET-to-NET, a única diferença está na ACL, já que é ela que define os pacotes a serem criptografados. Por exemplo, para estabelecer um túnel IPsec entre as redes 192.168.10.0 e 192.168.12.0, configura-se a seguinte ACL no roteador da rede 192.168.10.0 que se comunica com o roteador da rede 192.168.12.0.

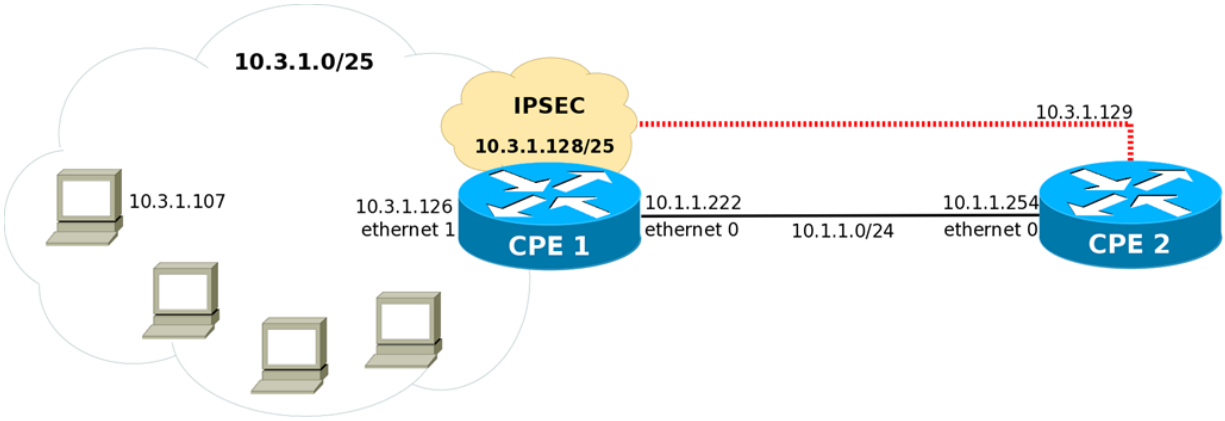
access-list 198 permit ip 192.168.10.0 0.0.0.255 192.168.12.0 0.0.0.255

É evidente que no outro peer é necessária uma configuração compatível. Caso for um roteador Digistar, pode-se utilizar a mesma ACL, entretanto, trocam-se os endereços IP das redes de origem e destino:

access-list 198 permit ip 192.168.12.0 0.0.0.255 192.168.10.0 0.0.0.255

4.14.4.4. VPN/Roadwarrior

Suponha o seguinte cenário:



O CPE 1 distribui endereços IP e o CPE 2 requisita (Roadwarrior). A ACL para o CPE 1, neste cenário é:

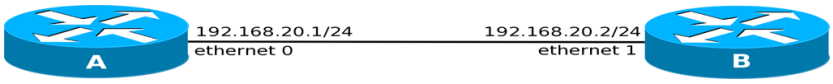
access-list 199 permit ip 10.3.1.0 0.0.0.127 host 10.1.1.254

Já para o CPE 2:

access-list 199 permit ip host 10.1.1.254 10.3.1.0 0.0.0.127

4.14.5. Exemplos de Configuração usando PSK

4.14.5.1. HOST-to-HOST



HOST A (Digistar):

```
crypto-isakmp key teste123 address 192.168.20.2
crypto isakmp policy 1
 encryption aes-256
 group 14
 hash md5
!
crypto ipsec transform-set tset esp-auth md5-hmac esp-cipher aes-256
crypto map SECURE 1 ipsec-isakmp
 authentication pre-share
 match 155
 set identity ID
 set peer 192.168.20.2
 set pfs group14
 set transform-set tset
 connection on-demand
 version ikev1
!
interface ethernet 0
 crypto map SECURE
!
access-list 155 permit ip host 192.168.20.1 host 192.168.20.2
```

HOST B (Digistar):

```
crypto-isakmp key teste123 address 192.168.20.1
crypto isakmp policy 1
 encryption aes-256
 group 14
 hash md5
!
crypto ipsec transform-set tset esp-auth md5-hmac esp-cipher aes-256
crypto map SECURE 1 ipsec-isakmp
 authentication pre-share
 match 199
 set identity ID
 set peer 192.168.20.1
 set pfs group14
 set transform-set tset
 connection on-demand
 version ikev1
!
interface ethernet 1
 crypto map SECURE
!
access-list 199 permit ip host 192.168.20.2 host 192.168.20.1
```

4.14.5.2. NET-to-NET

Para um cenário semelhante ao item anterior, mas com uma rede 10.1.1.0/24 atrás de A e 20.2.2.0/24 atrás de B, mudam-se, em relação à configuração anterior, apenas as ACLs:

HOST A (Digistar):

```
access-list 155 permit ip 10.1.1.0 0.0.0.255 20.2.2.0 0.0.0.255
```

HOST B (Digistar):

```
access-list 199 permit ip 20.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
```

4.14.5.3. VPN

Para o mesmo cenário da seção VPN/Roadwarrior.

CPE 1 (Digistar):

```
crypto isakmp key key address 10.1.1.254
crypto isakmp policy 1
 encryption 3des
 group 2
 hash sha
!
crypto ipsec transform-set tset esp-auth sha-hmac esp-cipher des
crypto map VPN 1 ipsec-isakmp
 authentication pre-share
 match 199
 set ip-address 10.3.1.128/25 10.3.1.126
 set peer 10.1.1.254
 set pfs group1
 set transform-set tset
 connection on-demand
 version ikev1
!
interface ethernet 0
 ip address 10.1.1.222 255.255.255.0
 crypto map VPN
!
interface ethernet 1
 ip address 10.3.1.126 255.255.255.128
 dhcp-server
  range 10.3.1.1 10.3.1.125
  gateway 10.3.1.126
  mask 255.255.255.128
 !
!
access-list 199 permit ip 10.3.1.0 0.0.0.127 host 10.1.1.254
```

CPE 2 (Digistar):

```
crypto isakmp key key address 10.1.1.222
crypto isakmp policy 1
 encryption 3des
 group 2

 hash sha
!
crypto ipsec transform-set tset esp-auth sha-hmac esp-cipher des
crypto map VPN 1 ipsec-isakmp
 authentication pre-share
 match 199
 set ip-address request
 set peer 10.1.1.222
 set pfs group1
 set transform-set tset
 connection always
 version ikev1
!
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
 crypto map VPN
!
access-list 199 permit ip host 10.1.1.254 10.3.1.0 0.0.0.127
```

4.14.6. Chaves RSA

Chaves RSA constituem uma peça fundamental para IPsec. São elas que possibilitam a segurança do IPsec. Quanto maior a chave, mais difícil de alguém comprometer a autenticidade, integridade e confidencialidade da informação. São usadas nos certificados também.

4.14.6.1. Gerando Novas Chaves

Para gerar uma nova chave RSA, use os comandos abaixo:

Tabela 152: Gerando Chaves RSA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto key generate rsa general-purpose [exportable] [modulus bits]label name **Exemplo:** CPE(config)#crypto key generate rsa general-purpose exportable modulus 1024 label mykey	Gera uma chave de rótulo name, de tamanho bits e opcionalmente exportável. O exemplo gera uma chave exportável mykey de 1024 bits e exportável.

4.14.6.2. Exportando Chaves

Para que seja possível exportar uma chave, ela deve ser do tipo exportável (exportable).

Tabela 153: Exportando Chaves RSA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto key export rsa name pem terminal{ des | 3des } pass **Exemplo:** Germano(config)#crypto key export rsa mykey pem terminal des teste123 Key name: mykey Usage: General Usage Key Key data: -----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEB.... (CONTINUA) -----END PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-CBC,1715F17A30C1950C nc1KhtTS/PwUH3m2JmYeUX... (CONTINUA) -----END RSA PRIVATE KEY-----	Exporta uma chave de rótulo name para o terminal, cifrando-a usando o algortimo des ou 3des com senha pass. O exemplo exporta a chave mykey do item anterior para o terminal, usando algoritmo des e senha teste123.

4.14.6.3. Importando Chaves

Para importar uma chave RSA, use os comandos abaixo:

Tabela 154: Importando Chaves RSA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto key import rsa name general-purpose [exportable] terminal pass	Importa a chave colada no terminal para o rótulo name, usando a senha de criptografia pass e sendo, opcionalmente exportável.

4.14.6.4. Excluindo Chaves

Para excluir uma chave RSA, use os comandos abaixo:

Tabela 155: Excluindo Chaves RSA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto key zeroise name	Remove a chave de rótulo name.

4.14.7. Certificados X.509

Usar certificados para IPsec é uma prática bastante comum e segura. Siga os itens abaixo para configurar trustpoints e obter certificados para o uso com IPsec.

4.14.7.1. Configurando Trustpoints

Um trustpoint é o elemento chave de configuração de certificados. Um trustpoint possui um nome e está sempre associado a uma CA (Autoridade Certificadora). Para cada trustpoint, pode-se obter um certificado diferente (cada um de uma CA). Na configuração de Crypto-Maps, utiliza-se o nome do trustpoint para se referir ao certificado a ser usado.

Tabela 156: Configurando Trustpoints

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca trustpoint name	Cria um trustpoint de nome name e entra no diretório de configuração do mesmo.
4	CPE(config-ca-trustpoint)#auto-enroll [percentage]	(OPCIONAL) Apenas para obtenção de certificado no modo Online, configura a renovação automática do certificado para percentage de sua vida útil.
5	CPE(config-ca-trustpoint)#crl url	(OPCIONAL) Configura CRL com a url.
6	CPE(config-ca-trustpoint)#enrollment { A.B.C.D | terminal }	Configura como será feita a obtenção do certificado associado a este trustpoint. Se por terminal (Offline) ou utilizando um endereço IPv4 (Online, via protocolo SCEP).
7	CPE(config-ca-trustpoint)#ocsp url	(OPCIONAL) Configura OCSP com a url.
8	CPE(config-ca-trustpoint)#rsakeypair label	Associa uma chave de rótulo label a este trustpoint.
9	CPE(config-ca-trustpoint)#subject-name dn **Exemplo:** CPE(config-ca-trustpoint)#subject-name c=BR,st=RS,cn=Digistar,l=Sao Leopoldo	Configura a identificação deste roteador, para ser incluída no certificado. Importante: veja abaixo os campos aceitos para inclusão no subject-name. O exemplo configura o subject-name com país BR, estado RS, nome comum Digistar e localidade Sao Leopoldo.
10	CPE(config-ca-trustpoint)#vrf name	(OPCIONAL) Configurada a vrf que o trustpoint é acessível (para obtenção de certificados online).

Campos aceitos para subject-name: businessCategory, c, cn, dc, description, destinationIndicator, distinguishedName, dnQualifier, enhancedSearchGuide, facsimileTelephoneNumber, generationQualifier, givenName, houseIdentifier, initials, internationalISDNNumber, l, member, name, o, ou, owner, physicalDeliveryOfficeName, postalAddress, postalCode, postOfficeBox, preferredDeliveryMethod, registeredAddress, roleOccupant, searchGuide, seeAlso, serialNumber, sn, st, street, telephoneNumber, teletexTerminalIdentifier, telexNumber, title, uid, uniqueMember, userPassword, x121Address, x500UniqueIdentifier, applicationProcess, country, dcObject, device, groupOfNames, groupOfUniqueNames, locality, organization, organizationalPerson, organizationalRole, organizationalUnit, person, residentialPerson, uidObject, unstructuredName.

Nota: Equipamentos Cisco podem incluir o campo unstructuredName em seus certificados sem que a configuração seja feita. Normalmente o valor deste campo é o hostname do roteador. Isso deve ser levado em conta na hora de configurar uma restrição de identidade para uma conexão estes. Sem este campo a conexão não será estabelecida corretamente.

4.14.7.2. Obtenção de Certificado Offline

A obtenção de certificados offline pode ser dividida em três passos. O primeiro consiste em configurar um trustpoint. Este trustpoint deve ser configurado com enrollment terminal. Por exemplo:

```
crypto ca trustpoint mytp
 vrf global
 subject-name C=BR,ST=RS,CN=Digistar,O=Digistar SA,OU=Engenharia
enrollment terminal
 rsakeypair mykey
!
```

O segundo passo é importar o certificado da autoridade certificadora:

Tabela 157: Autenticando um Trustpoint

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca authenticate name **Exemplo:** CPE(config)#crypto ca authenticate mytp Enter the base 64 encoded CA certificate. (COLAR O CERTIFICADO AQUI) --- BEGIN ..... 0123456789ABCDEF..... --- END	Importa o certificado da autoridade certificador (colar no terminal). O exemplo importa o certificado da CA associada ao trustpoint mytp.

O terceiro passo é gerar a requisição do certificado.

Tabela 158: Gerando uma Requisição de Certificado

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca enroll name	Gera a requisição do certificado. Ela será mostrada no console. Esta requisição deve ser enviada à CA.

Após a CA receber a requisição e emitir o certificado, deve ser feita a importação deste. Isso pode ser feito imediatamente após o comando anterior, ou mais tarde. Após a execução do comando anterior, o equipamento irá perguntar se deseja importar o certificado imediatamente ou mais tarde. Caso se responda não, para importar mais tarde, deve ser usado o comando explicado mais adiante no item “Importando Certificados”. Caso se responda sim, basta colar o certificado no console.

4.14.7.3. Obtenção de Certificado Online (SCEP)

O protocolo SCEP automatiza a obtenção de certificado. Para se obter um certificado de forma online, basta configurar um trustpoint com "enrollment <Endereço IP>", como mostrado abaixo e executar mais dois simples passos. Exemplo de trustpoint:

```
crypto ca trustpoint mytp
 vrf global
 subject-name C=BR,ST=RS,CN=Digistar,O=Digistar SA,OU=Engenharia
enrollment 192.168.11.1
 rsakeypair mykey
!
```

Configurado o Trustpoint, assim como no offline, deve-se importar o certificado da CA, gerar a requisição de certificado, enviar esta requisição para a CA e importar o certificado gerado pela CA. Com o protocolo SCEP, isso tudo fica extremamente simples.

Tabela 159: Obtendo Certificado Online via SCEP

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca autenticate name	Obtém o certificado da CA associada ao trustpoint name.
4	CPE(config)#crypto ca enroll name	Gera a requisição, envia à CA, recebe e importa o certificado gerado.

4.14.7.4. Importando Certificados

Para importar um certificado associado a um trustpoint, usa-se os comandos abaixo. É utilizado para importar manualmente certificados, geralmente offline.

Tabela 160: Importando Certificados Manualmente.

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca import name certificate	Importa o certificado gerado pela CA.

4.14.7.5. Exportando Certificados

Para exportar um certificado associado a um trustpoint, use os comandos abaixo:

Tabela 161: Exportando Certificados

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#crypto ca export certificate	Exporta o Certificado.

4.14.7.6. Configurações Extras

Estas configurações são na maioria das vezes opcionais ou necessárias apenas para interoperabilidade com equipamentos não Digistar.

4.14.7.6.1. ISAKMP Identity

Configura como o equipamento deve se identificar quando usa o protocolo ISAKMP. As opções são:

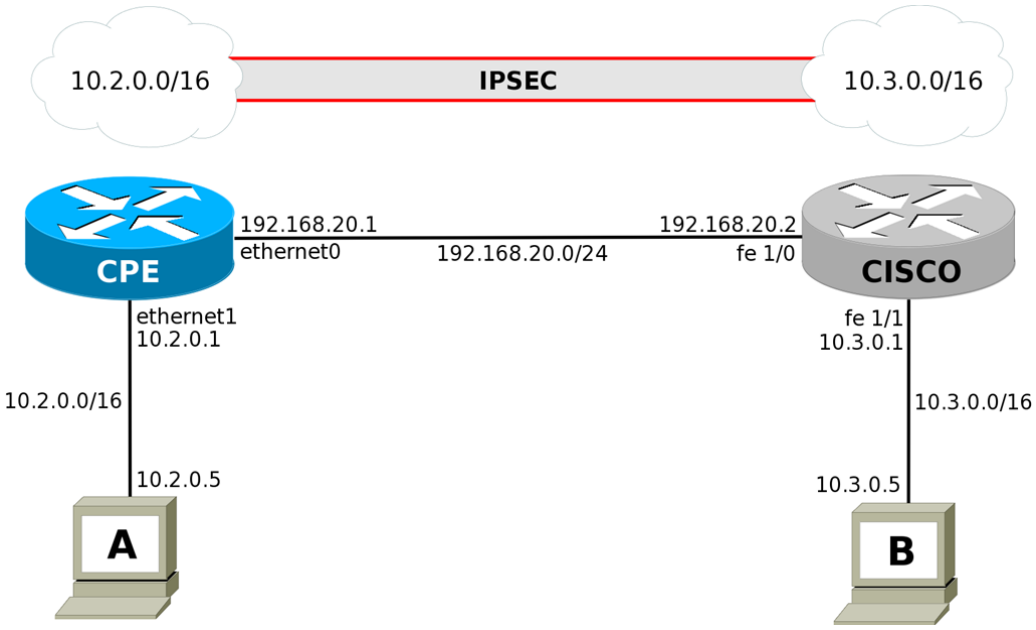
address: usar o endereço IP da interface de saída
dn: usar o DN do certificado (configuração padrão e recomendada)
hostname: usar o hostname do roteador

4.14.7.6.2. Restrição de Identidade

Para realizar uma conexão IPsec com certificados, pode ser necessário explicitar o DN do outro peer. A configuração é feita da mesma forma e com os mesmos campos válidos do subject-name do trustpoint.

4.14.8. Exemplos de Configuração usando Certificados

4.14.8.1. Interoperabilidade CISCO (Certificados)



CPE (Digistar):

```
crypto identity ID
 dn CN=CISCO,OU=Engenharia,O=Digistar,ST=RS,C=BR,unstructuredName=Cisco
!
crypto isakmp policy 1
 encryption 3des
 group 2
 hash md5
!
crypto ipsec transform-set tset esp-auth md5-hmac esp-cipher 3des
crypto map SECURE 1 ipsec-isakmp
 authentication certificate mytp
 match 199
 set identity ID
 set peer 192.168.20.2
 set transform-set tset
 set pfs group2
 connection on-demand
 version ikev1
!
```

```
interface ethernet 0
 ip address 192.168.20.1 255.255.255.0
 crypto map SECURE
 no shutdown
!
interface ethernet 1
 ip address 10.2.0.1 255.255.255.0
 no shutdown
!
access-list 199 permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255

ip route 10.1.1.0/24 192.168.10.200
ip route 10.3.0.0/16 192.168.20.2
```

CISCO:

```
crypto isakmp policy 1
 encr 3des
 hash md5
 group 2
!
crypto isakmp identity dn
crypto ipsec transform-set tset esp-3des esp-md5-hmac
!
crypto map SECURE 1 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set tset
 match address 111
!
interface Ethernet1/0
 ip address 192.168.20.2 255.255.255.0
 crypto map SECURE
 duplex full
 no shutdown
!
interface Ethernet1/1
 ip address 10.2.0.1 255.255.255.0
 duplex full
 no shutdown
!
ip route 10.2.0.0 255.255.0.0 192.168.20.1
access-list 111 permit ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

4.15. PKI Server

(recurso habilitado por licença)

O PKI server é uma ferramenta para configuração de CA no roteador Digistar.

4.15.1. Criando um Offline PKI Server

A funcionalidade de Offline PKI Server provê a configuração de uma CA para obtenção de certificados por terceiros, de forma offline. Para configurar, siga os passos abaixo:

Tabela 162: Configuração de PKI Server

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# crypto ca server	Entra no diretório de configuração do PKI Server.
4	CPE(config-ca-server)#cdp-url url	(OPCIONAL) Configura uma URL de CRL para ser incluída nos certificados gerados.
5	CPE(config-ca-server)#grant { auto | none }	(OPCIONAL) Configura para os certificados serem emitidos imediatamente (sem autorização) ou negados imediatamente.
6	CPE(config-ca-server)#issuer-name dn	Configura o DN da CA, da mesma forma que o subject-name do trustpoint.
7	CPE(config-ca-server)#lifetime ca-certificate days	(OPCIONAL) Validade do certificado da CA
8	CPE(config-ca-server)#lifetime certificate days	(OPCIONAL) Validade dos certificados gerados
9	CPE(config-ca-server)#lifetime crl days	(OPCIONAL) Validade da CRL gerada
10	CPE(config-ca-server)#rsakeypair label	Rótulo da chave a ser usada na confecção do certificado desta CA
11	CPE(config-ca-server)#serial-number num	(OPCIONAL) Número de série atual dos certificados emitidos.
12	CPE(config-ca-server)#no shutdown	Inicia o servidor. Nenhuma configuração pode ser alterada após este passo.

Após a correta execução destes passos, o servidor PKI estará operacional. O certificado desta CA será gerado. É importante que as configurações de data e hora estejam corretas (preferencialmente com NTP).

4.15.2. Exportando o Certificado desta CA

Para que se autentique trustpoints em outros equipamentos, é necessário que eles importem o certificado desta CA. Para que eles importem, é necessário exportar usando os comandos abaixo:

Tabela 163: Exportando Certificado da CA

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# crypto ca export certificate	Exporta o certificado.

4.15.3. Coletando uma Requisição

Após a configuração do servidor PKI, é possível receber requisições de certificados e emitílos. Para isso, siga os passos abaixo:

Tabela 164: Coletando uma Requisição

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server request	Recebe uma requisição via terminal (colar). Dependendo da configuração do servidor, o certificado será emitido imediatamente ou precisará antes ser autorizado.

4.15.4. Autorizando uma Requisição

Para emitir um certificado de uma requisição pendente, use os comandos abaixo.

Tabela 18: Autorizando uma Requisição

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server grant { ID | all }	Autoriza a requisição e exporta o certificado para o terminal. Pode ser de uma requisição única ID ou todas (all).

4.15.5. Excluindo todas as Requisições

Para limpar todas requisições, use os comandos abaixo.

Tabela 165: Limpando a base de requisições

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server cleanup	Limpa todas as requisições.

4.15.6. Excluindo uma Requisição

Para limpar todas as requisições, use os comandos abaixo.

Tabela 166: Excluindo uma Requisição

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server remove { ID | all }	Exclui a requisição específica ID ou todas as requisições (all).

4.15.7. Revogando um Certificado

Para limpar todas as requisições, use os comandos abaixo.

Tabela 167: Autorizando uma Requisição

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server revoke serial	Emite o certificado de revogação do certificado de número de série serial

4.15.7.1. Revalidando um Certificado Revogado

Quando um certificado é revogado por engano, ele pode ser revalidado.

Tabela 168: Autorizando uma Requisição

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE#crypto ca server unrevoke serial	Caso o um certificado tenha sido revogado e se queira desfazer esta ação, usar o comando ao lado para cada certificado de número de série serial.

4.16. Conection Fault Management (IEEE802.1ag)

(recurso habilitado por licença)

4.16.1. Considerações Iniciais

O equipamento Digistar suporta o protocolo CFM como MEP. Portanto, pode ser usado na borda da rede Metro Ethernet, no MD de mais alto nível. As funcionalidades de MIP não são suportadas, assim como o padrão ITU-T Y.1731.

4.16.1.1. Configuração

Para ativar o CFM, deve-se habilitá-lo tanto globalmente como e em cada interface em que se deseja que ele envie e receba LTMs, LTRs, LBMs, LBRs e CCMs. O primeiro passo é habilitá-lo, depois configuram-se domínios e por último os MEPs nas interfaces.

4.16.1.2. Habilitando o CFM

Sem habilitar o CFM globalmente, nenhuma funcionalidade do protocolo é ativada. Para habilitar globalmente, use os comandos da tabela abaixo. Porém, apenas habilitá-lo globalmente não ativa nenhuma funcionalidade, outras configurações são necessárias.

Tabela 169: Configuração de CFM global

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ethernet cfm global	Habilita o CFM globalmente.

4.16.1.3. Configurando um Domínio

O MD é uma configuração fundamental do CFM. Para configurá-lo, use os comandos da tabela abaixo. Também é necessário configurar pelo menos um serviço no domínio.

Tabela 170: Configuração de Domínio

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ethernet cfm domain *name* level *num* **Exemplo:** CPE(config)# ethernet cfm domain example level 5	Acessa o modo de configuração do dominio. **Parâmetros:** *name:* nome do MD *num*: nível do MD O exemplo cria e acessa o modo de configuração do domínio “example” de nível 5.
4	CPE(config-ecfm)# description	(Opcional) Configura uma descrição para o MD.
5	CPE(config-ecfm)#mep archive-hold-time *minutes* **Exemplo:** CPE(config-ecfm)# mep archive-hold-time 200	(Opcional) Configura um *timeout* para lembrar os MEPs remotos do domínio. **Parâmetros:** *minutes:* tempo em minutos O exemplo configura para 200 minutos.
6	CPE(config-ecfm)#sender-id chassis	(Opcional) Configurar para enviar o número do equipamento como sender-id. Esta é a configuração padrão para todos os serviços deste domínio que não possuirem configuração específica de sender-id.

4.16.1.3.1. Configurando um Serviço no Domínio

Para configurar um serviço em um domínio já existente, siga os comandos da tabela abaixo.

Tabela 171: Configuração de Serviço

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ethernet cfm domain *name* level *num* **Exemplo:** CPE(config)# ethernet cfm domain example level 5	Acessa o modo de configuração do dominio. O exemplo acessa o modo de configuração do domínio “example” de nível 5, criado anteriormente.
4	CPE(config-ecfm)# service *name* vlan *tag* direction down **Exemplo:** CPE(config-ecfm)# service customer1 vlan 100 direction down	Entra no modo de configuração de serviço no domínio. **Parâmetros:** *name:* tempo em minutos *tag*: tempo em minutos O exemplo cria e acessa o modo de configuração do domínio “example” de nível 5.
5	CPE(config-ecfm-srv)#continuity-check	(Opcional) Habilita o envio e recebimento de CCMs.
6	CPE(config-ecfm-srv)#continuity-check interval *interval* **Exemplo:** CPE(config-ecfm-srv)# continuity-check interval 100ms	(Opcional) Configura o intervalo entre cada CCM. **Parâmetros:** *interval:* tempo O exemplo configura para transmissão de CCMs a cada 100ms.
7	CPE(config-ecfm-srv)#continuity-check loss-threshold *messages* **Exemplo:** CPE(config-ecfm-srv)#continuity-check loss-threshold 10	(Opcional) Configura o limiar de perda de CCMs. **Parâmetros:** *messages:* número de mensagens esperadas de acordo com o intervalo configurado. O exemplo configura para 10 mensagens
8	CPE(config-ecfm-srv)#description *text*	(Opcional) Configura uma descrição para o serviço.

9	CPE(config-ecfm-srv)#maximum meps *num* **Exemplo:** CPE(config-ecfm-srv)#maximum meps 20	(Opcional) Configura um número máximo de MEPs remotos para o serviço. **Parâmetros:** *num:* número de MEPs O exemplo configura para 20.
10	CPE(config-ecfm-srv)#sender-id { chassis | none } **Exemplo:** CPE(config-ecfm-srv)#sender-id none	(Opcional) Configura o envio de sender-id nos pacotes. Esta configuração se sobrepõe a do domínio. **Parâmetros:** chassis: número do equipamento none: não envia O exemplo configura para não enviar.

4.16.1.4. Configurando um MEP

Para configurar um MEP ativo, deve-se habilitar o CFM na interface e instalar um MEP.
O CFM deve estar globalmente habilitado.

4.16.1.4.1. Habilitar CFM na Interface

Para habilitar o CFM na interface, siga os comandos da tabela abaixo.

Tabela 172: Habilitar CFM na interface

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *type number* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ethernet cfm interface	Habilita CFM na interface.

4.16.1.4.2. Configurar um MEP na Interface

Para configurar um MEP na interface, siga os comandos da tabela abaixo. Um domínio com serviço deve ter sido previamente configurado. Para que o MEP envie e receba mensagens CFM, a interface VLAN correspondente ao serviços do domínio deve estar configurada e ligada.

Tabela 173: Habilitar um MEP na interface

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *type number* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ethernet cfm mep domain *domain* mpid *id* { service *service* | vlan *vlan }* **Exemplo:** *CPE(config)# e*thernet cfm mep domain example mpid 123 service customer1.	Configura um MEP na interface. **Parâmetros:** *domain*: nome do MD *id*: ID do MEP *service*: nome do serviço *vlan*: número da VLAN O exemplo configura um MEP no domínio *example*, com MEP ID 123 e serviço “customer1”.

4.16.1.5. Configurando Alarmes

Podem ser gerados alarmes para defeitos detectados pelo CFM. Estes alarmes são reportados via SNMP e também podem ser visualizados via linha de comando.

4.16.1.5.1. Tempo de Atraso do Alarme

Para configurar utilize os comandos da tabela abaixo:

Tabela 174: Atraso do Alarme do CFM

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#ethernet cfm alarm delay *time* **Exemplo:** CPE(config)# ethernet cfm alarm delay 4000	Configura o tempo que um defeito deve persistir para que um alarme seja emitido. **Parâmetros:** *time*: tempo em ms. O exemplo configura para 4000ms.

4.16.1.5.2. Notificações

Nem todos defeitos detectados pelo CFM precisam gerar alarmes. O administrador pode definir a gravidade mínima dos defeitos que geram alarmes. Para configurar utilize os comandos da tabela abaixo:

Tabela 175: Notificações do CFM

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#ethernet cfm alarm notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon } **Exemplo:** CPE(config)# ethernet cfm alarm notification all	Configura os defeitos que geram alarmes. O exemplo configura que todos os defeitos devem gerar alarmes.

4.16.1.5.3. Tempo para Limpar os Alarmes

Depois que um alarme é disparado, o defeito deve desaparecer por um determinado tempo para que o alarme possa ser disparado novamente. Para configurar este tempo utilize os comandos da tabela abaixo:

Tabela 176: Limpar Alarmes do CFM

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#ethernet cfm alarm reset *time* **Exemplo:** CPE(config)# ethernet cfm alarm reset 3500	Configura por quanto tempo um defeito deve deixar de existir para que o alarme seja reiniciado. **Parâmetros:** *time*: tempo em ms. O exemplo configura para 3500ms.

4.16.2. Estatísticas

O equipamento digistar fornece informações de configuração, erros e estatísticas do protocolo CFM.

4.16.2.1. Defeitos

Para mostrar os defeitos detectados ou reportados por outros MEPs, utilize o comando:

```
Digistar-CPE#show ethernet cfm errors

Interface ethernet1
  Vlan 100 MEPID 123
    Remote MEPID 2
      Current errors:
        DefRDI - remote defect indication
      Past errors:
        None
```

4.16.2.2. MEPs Locais e Remotos

Existem dois comandos para exibir MEPs. Um para MEPs configurados localmente e outro para MEPs descobertos via *heartbeats* de CCM.

4.16.2.2.1. Mostrar MEPS Locais Ativos

Utilize o comando:

```
Digistar-CPE#show ethernet cfm maintenance-points local
Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                Lvl  MacAddress        Type   CC
Ofld Domain Id                                  Dir  Port              Id
     MA Name                                         SrvcInst          Source
     CC-Interval                                     CC-Threshold      CoS
     EVC name                                        RemMeps/Max
--------------------------------------------------------------------------------
123  example                                    5    00:D0:10:05:15:44 Vlan   Y
No   example                                    Down ethernet1         100
     digistar                                        N/A               Static
     10 seconds                                      3                 0
     N/A                                             1/100

Total Local MEPs: 1
```

4.16.2.2.2. Mostrar MEPS Remotos

Utilize o comando:

```
Digistar-CPE#show ethernet cfm maintenance-points remote
-------------------------------------------------------------------------------
MPID  Domain Name                                MacAddress          IfSt  PtSt
 Lvl  Domain ID                                  Ingress
 RDI  MA Name                                    Type Id             SrvcInst
      EVC Name                                   Age
-------------------------------------------------------------------------------
2     example                                    00:21:A0:7D:1E:B0    Up    Up
   5  example                                    ethernet1
 Yes  digistar                                   Vlan 100            N/A
      N/A                                        1s

Total Remote MEPs: 1
```

4.16.2.3. Estatísticas de Pacotes CFM

Para exibir estatísticas de pacotes CFM, utilize o comando abaixo:

```
Digistar-CPE#show ethernet cfm statistics

Interface ethernet1 MPID 123:
  CCMs:
    Transmitted:                 7   Received:                 7
    Remote MEP    2 Received Sequence Errors:                  0
  LTRs:
    Received:                    0   Replied:                  0
  LBRs:
    Received:                    0   Replied:                  0
  Last clearing of counters: never
```

4.17. Ethernet Local Management Interface (E-LMI)

(recurso habilitado por licença)

Esta seção trata da configuração das funcionalidades do protocolo E-LMI, definido pelo *Metro Ethernet Forum** na especificação técnica MEF 16. Detalhes conceituais e a terminologia empregada podem ser encontrados tanto na MEF 16 quanto em outros documentos aprovados pelo MEF.

http://metroethernetforum.org/

4.17.1. Considerações Iniciais

O equipamento Digistar suporta o protocolo E-LMI do lado CE. Ou seja, ele recebe informações do PE e com estas informações é capaz de:

- manter comunicação via E-LMI com o PE.
- Receber informações de EVCs
- habilitar e desabilitar interfaces VLAN
- configurar bandwidth profiles

Ao se habilitar o E-LMI, todas interfaces VLAN filhas são bloqueadas e se comportam como se estivessem no estado “down”. Dependendo das informações recebidas do PE, o LMI pode habilitar estas interfaces e configurar alguns de seus parâmetros. Entretanto, é fundamental que o administrador já tenha criado estas interfaces no configurador.

É bom lembrar que o E-LMI pode bloquear, desbloquear ou reconfigurar as interfaces a qualquer momento, de acordo com os dados recebidos do PE. Algumas configurações, se ativas, são mostradas no comando “show interface”.

O E-LMI é apenas suportado em portas ethernet roteadas, não sendo suportado nas portas Switch pois as mesmas não são roteadas.

4.17.2. Configuração de E-LMI

A configuração do E-LMI pode ser divida em duas partes: habilitar E-LMI na interface e configurar os parâmetros. Para habilitar na interface, pode-se habilitar uma a uma ou usar a configuração global e habilitar em todas ao mesmo tempo. Já a configuração dos parâmetros deve ser feita individualmente em cada interface.

4.17.2.1. Configuração Global

Este comando habilita E-LMI em todas as interfaces suportadas.

Tabela 177: Configuração de E-LMI Global

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# ethernet lmi global	Habilita E-LMI em todas as interfaces suportadas.

4.17.2.2. Configuração na Interface

Dentro das interfaces é possível habilitar o E-LMI apenas para a interface e também ajustar os parâmetros do protocolo.

4.17.2.2.1. Habilitar E-LMI na Interface

Este comando habilita o E-LMI em uma interface específica.

Tabela 178: Configuração de E-LMI na interface

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *type number* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ethernet lmi interface	Habilita E-LMI na interface.

4.17.2.2.2. Parâmetros do E-LMI na Interface

Os parâmetros relativos a CE podem ser configurados. São eles: N391, N393 e T391. Para voltar aos valores padrão, utilize a forma 'no' do comando.

Tabela 179: Configuração de parâmetros E-LMI na interface

Passo	Comando	Objetivo
1	CPE> enable	Habilita o usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# interface *type number* **Exemplo:** CPE(config)# interface ethernet 1	Acessa o modo de configuração da interface. O exemplo acessa o modo de configuração da interface ethernet 1.
4	CPE(config-interface)# ethernet lmi n391 *counter* **Exemplo:** *CPE(config-interface)# ethernet lmi n391 30*	(Opcional) Configura o parâmetro N391. **Parâmetros:** *counter:* contador de 1 a 65535 O exemplo configura n391 para 30.
5	CPE(config-interface)# ethernet lmi n393 *counter* **Exemplo:** *CPE(config-interface)# ethernet lmi n393 2*	(Opcional) Configura o parâmetro N393; **Parâmetros:** *counter:* contador de 1 a 10 O exemplo configura n393 para 2.
6	CPE(config-interface)# ethernet lmi t391 *counter* **Exemplo:** *CPE(config-interface)# ethernet lmi t391 10*	(Opcional) Configura o parâmetro T391. **Parâmetros:** *counter:* contador de 5 a 30. O exemplo configura T391 para 10.

4.17.3. Mostra de Estatísticas e Configurações

O E-LMI possui três commandos de *shows*. O primeiro mostra as informações de EVCs recebidas do PE em cada interface.

Nota: no campo VLANs, aparecem as ce-vlans informadas pelo PE. As que não estiverem criadas no equipamento *Digistar* aparecem como "(Not Configured)".

```
Digistar#show ethernet lmi evc
Interface: ethernet1
  Ether LMI Link Status: Up
  UNI Id: ME-3400-FE0/13
  EVC Id: myevc
    EVC Status: Inactive
    EVC Type: Point-to-Point
    Default EVC: No
    VLANs:       100 (Not Configured)
    Remote UNI Count: Configured =  1, Active = 0
    CIR : Undefined
    CBS : Undefined
    EIR : Undefined
    EBS : Undefined
    Untagged and Priority Service: No
```

Já o segundo comando mostra os parâmetros E-LMI das interfaces:

```
CPE-Germano#show ethernet lmi parameters


E-LMI Parameters for interface ethernet0
  Mode : CE
  T391 : 10
  N391 : 360
  N393 : 4
```

E o terceiro informa as estatísticas de pacotes E-LMI.

```
CPE-Germano#show ethernet lmi statistics
E-LMI Statistics for interface ethernet1
  Ether LMI Link Status: Up
  UNI Status: Up
  UNI Id: ME-3400-FE0/13

  Sequence Numbers:
    Send                          67  Receive                       67

  Reliability Errors:
    Status Enq Timeouts            2  Invalid Sequence Number        0

  Protocol Errors:
    Invalid Protocol Version       0  Invalid EVC Reference Id       0
    Invalid Message Type           0  Unexpected IE                  0
    Invalid Mandatory IE           0  Invalid non-Mandatory IE       0
    Short Message                  2  Other                          0

  Last clearing of counters        never
```

4.18. Serviços

4.18.1. HTTP

A tabela a seguir mostra os procedimentos para configuração do servidor HTTP (RFC 2616):

Tabela 180: Configuração do servidor HTTP.

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] ip http server	Habilita ou desabilita o servidor HTTP.
4	CPE (config)# ip http port port-number	Define a porta do HTTP (de 1025 até 65535). A porta default é a 80. Para remover a configuração, usa-se: **no ip http port**
5	CPE (config)# ip http realm realm-string	Define a string para autenticação no HTTP (RFC 2617). Para remover a configuração usa-se: no ip http realm
6	CPE (config)# [no] ip http secure-server	Habilita ou desabilita o servidor HTTPS (RFC 2818).
7	CPE (config)# ip http secure-port port-number	Define a porta do HTTPS (de 1025 até 65535). A porta default é a 443. Para remover a configuração, usa-se: **no ip http secure-port**

4.18.2. SSH

A tabela a seguir mostra os procedimentos para configuração do servidor SSH (RFC 4251):

Tabela 181: Configuração do servidor SSH

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] ip ssh server	Habilita ou desabilita o servidor SSH
4	CPE (config)# ip ssh port port-number	Define a porta do SSH (de 1025 até 65535). A porta default é a 22. Para remover a configuração, usa-se: **no ip ssh port**

Comandos relacionados

CPE# ssh [user@]destination[:port] **Exemplo:** CPE# ssh suporte@192.168.1.2	Acessa um dispositivo via protocolo SSH. **Parâmetros:** **user:** Login do usuário. **destination:** Endereço IP ou nome do host de destino. **port:** Porta de destino. Se nenhum número de porta é especificado, é usada a porta 22.

4.18.3. TELNET

Abaixo são mostradas as configurações do servidor TELNET (RFC 854):

Tabela 182: Configuração do servidor TELNET

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# [no] ip telnet server	Habilita ou desabilita o servidor TELNET.
4	CPE (config)# ip telnet port port-number	Define a porta do TELNET (de 1025 até 65535). A porta default é a 23. Para remover a configuração, usa-se: **no ip telnet port**

Comandos relacionados

CPE# telnet [user@]destination[:port] **Exemplo:** CPE# telnet admin@192.168.1.10	Acessa um dispositivo via TELNET. **Parâmetros:** **user:** Login do usuário. **destination:** Endereço IP ou nome do host de destino. **port:** Porta de destino. Se nenhum número de porta é especificado, é usada a porta 23.

4.18.4. Simple Network Management Protocol – SNMP

O SNMP (Simple Network Management Protocol) (RFC 1157) (RFC 1905) (RFC 2571) permite aos administradores de rede gerenciar os equipamentos e diagnosticar problemas. Sua arquitetura baseia-se em três elementos: dispositivos gerenciados, agentes e sistemas de gestão de redes (ou gerentes). Um dispositivo gerenciado coleta informações (como por exemplo, endereços IP das interfaces) e roda um agente SNMP, que por sua vez disponibiliza estas informações respondendo as consultas realizadas pelo sistema de gestão de redes.

As solicitações partem sempre do sistema de gestão, que pode ser instalado em servidores e/ou na máquina do administrador da rede. Além de responder as consultas, o agente pode enviar notificações (conhecidas como traps) na ocorrência de mudanças no estado do dispositivo. As traps são enviadas sem que seja feita qualquer consulta, ou seja, este tipo de comunicação é feito exclusivamente por iniciativa do agente.

Na tabela abaixo são apresentados os procedimentos para configuração do agente SNMP nas versões 1 e 2 do protocolo.

Tabela 183: Configurações do SNMP v1 e v2.

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# snmp-server [vrf vrf-name] community *community-string* {ro | rw} [acl-number] **Exemplo:** CPE(config)# access-list 10 permit 192.168.2.0 0.0.0.255 CPE(config)# access-list deny any CPE(config)# snmp-server community admin ro 10	(Opcional) Habilita o agente SNMP, definindo uma string para a comunidade, podendo também configurar uma ACL. A opção **ro é** usada para configurar o direito de leitura de valores de objetos via SNMP. Já a opção **rw** configura o direito de leitura e alteração nos valores dos objetos. Também é possível definir uma ACL para restringir o acesso SNMP para uma determinada rede ou host. Podem ser usadas ACLS padrão (de 1 até 99 e de 1300 até 1399). No exemplo é configurada a string de comunidade **admin** com direito de leitura. Somente serão aceitas as requisições SNMP originadas na rede 192.168.2.0/24.

A tabela a seguir mostra as configurações do SNMP versão 3.

Tabela 184: Configurações do SNMP v3.

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração .
3	CPE(config)# snmp-server [vrf vrf-name] user *username* v3 auth {md5 | sha} *auth-word* [priv aes *passwd* | priv des *passwd*] **Exemplo:** CPE(config)# snmp-server user admin123v3 auth md5 adminpass1 priv aes privpass1	(Opcional) Configura um usuário para acesso ao agente SNMP, autenticação e opcionalmente, privacidade. **Parâmetros:** **md5:** Configura o uso de autenticação MD5. **sha:** Configura o uso de autenticação SHA. **auth-word**: Senha para autenticação, que deve ter no mínimo 8 caracteres. **priv aes:** Configura o uso de criptografia AES de 128 bits. **priv des:** Configura o uso de criptografia DES de 56 bits. **passwd:** Senha para criptografia, que deve ter no mínimo 8 caracteres. No exemplo é configurado o usuário **admin123** com autenticação MD5 e senha para autenticação **adminpass1**, habilitando o uso de criptografia AES, com a senha **privpass1**.

Abaixo são mostradas as configurações opcionais do SNMP, que podem ser usadas em todas as versões do protocolo.

Tabela 185: Configurações opcionais do SNMP

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração .
	CPE (config)# snmp-server chassis-id id-string	(Opcional) Configura um texto para identificar unicamente o agente SNMP. Para remover a configuração, usa-se: **no snmp-server chassis-id**
	CPE (config)# snmp-server contact contact-string	(Opcional) Configura um texto para o contato (sysContact). Para remover a configuração, usa-se: **no snmp-server contact**
	CPE (config)# snmp-server location location-string	(Opcional) Configura um texto para a localização do agente SNMP (sysLocation). Para remover a configuração, usa-se: **no snmp-server location**

CPE(config)# snmp-server host [vrf vrf-name] {*host-addr* | *host-name*} [global | host-vrf vrf-name] informs version 2c *community-string* udp-port *port*	(Opcional) As notificações SNMP podem ser enviadas na forma de traps ou de inform requests. A principal diferença entre estes dois tipos se dá pelo fato de as traps serem pouco confiáveis por que o receptor não envia confirmações de recebimento, ao contrário do que acontece com os inform requests. Além disso, os informs consomem mais recursos, visto que eles devem ficar armazenados até que a resposta seja recebida ou até que ocorra timeout, podendo ser feitas diversas re tentativas. As traps, por sua vez, são descartadas logo após o envio. A escolha de um ou outro tipo deve ser orientada pela criticidade da informação que é enviada e pela disponibilidade de recursos. O comando **snmp-server host informs** configura os hosts que devem receber os inform requests SNMP na versão 2c, definindo uma string de comunidade (que é enviada nas notificações) e a porta UDP (de 0 até 65535). **Importante: Este comando é válido somente para o SNMP versão 2c.** Para remover a configuração, usa-se: **no snmp-server {host-addr | host-name} informs**
CPE (config)# snmp-server host host-addr traps version {1 | 2c} community-string udp-port port	(Opcional) Configura os hosts que devem receber as traps SNMP nas versões 1 ou 2c, definindo uma string de comunidade (que é enviada nas notificações) e a porta UDP (de 0 até 65535). Para remover a configuração, usa-se: **no snmp-server {host-addr | host-name} traps version {1 | 2c}**
CPE (config)# [no] snmp-server trap authentication access-failures	(Opcional) Habilita/desabilita o envio de traps indicando a ocorrência de falha de autenticação. Nas versões1 ou 2c, ocorre falha de autenticação no recebimento de pacotes com a string de comunidade incorreta, enquanto que na versão 3, ocorre falha se a chave para autenticação SHA/MD5 é incorreta.
CPE (config)# [no] snmp-server trap link	(Opcional) Habilita/desabilita o envio de traps SNMP linkUp/linkDown, de acordo com a RFC 2233.

4.18.5. Syslog

O protocolo Syslog é utilizado para monitoramento e registro de mensagens do sistema, podendo ser utilizado para transmitir desde mensagens de caráter informativo até aquelas que são extremamente críticas. Cada mensagem enviada para o servidor Syslog possui dois rótulos descritivos associados, o que torna o processamento mais fácil. O primeiro rótulo informa a funcionalidade da aplicação que gerou a mensagem, enquanto que o segundo descreve em uma escala de 0 a 7 o quão crítica é a mensagem (emergência, alerta, debugging, etc.).

A tabela abaixo mostra os comandos para configuração do Syslog.

Tabela 186: Configurações do Syslog

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração global.
3	CPE (config)# [no] logging on	(Opcional) Habilita/desabilita o registro/envio de logs.
	CPE (config)# [no] logging buffered	(Opcional) Habilita/desabilita o armazenamento local das mensagens de log.
	CPE (config)# [no] logging console	(Opcional) Habilita/desabilita o envio de mensagens de log para o console.
	CPE (config)# logging facility facility-type	(Opcional) Configura as aplicações nas quais devem ser enviadas. **Opções:** **auth:** Autorização **cron:** Cron **daemon:** daemons **ftp:** FTP **kern**: Kernel **local0 – local7:** Local use **lpr:** Line printer system **mail:** Mail **news:** USENET news **syslog:** Syslog **user:** processos de usuário **uucp:**Unix-to-Unix copy system Para remover a configuração, usa-se: **no logging facility**

	CPE (config)# logging host {ipv4-addr | fqdn | ipv6-addr} transport udp port port-number	(Opcional) Configura o IP do servidor Syslog para o qual serão enviadas as mensagens de log, o protocolo de transporte (no caso, UDP) e a porta correspondente. Para remover a configuração, usa-se: **no logging host**
	CPE (config)# logging host {ipv4-addr | fqdn | ipv6-addr} vrf vrf-name transport udp port port-number	(Opcional) Configura o IP do servidor Syslog para o qual serão enviadas as mensagens de log, o nome da VRF onde se encontra o IP ou FQDN, o protocolo de transporte (no caso, UDP) e a porta correspondente. Para remover a configuração, usa-se: **no logging host**
	CPE (config)# logging origin-id {hostname | string id-string}	(Opcional) Configura um identificador para as mensagens que são enviadas para o servidor Syslog remoto. Pode ser usado o hostname ou uma string com texto único. Para remover a configuração, usa-se: **no logging origin-id**
	CPE (config)# logging trap level	(Opcional) Configura o envio de traps associadas a um determinado nível de severidade. **Parâmetros e opções:** **level:** Pode ser configurado diretamente um valor de 0 a 7 ou uma das severidades abaixo: **alerts:** Necessita de ação imediata (severidade = 1). **critical:** Indica que o sistema se encontra em condições críticas (severidade = 2). **debugging:** Mensagens de debug (severidade = 7). **emergencies:** Não é possível utilizar o sistema (severidade = 0). **errors:** Indica condição de erro (severidade=3) . **informational:** Mensagem informativa (severidade=6). **notifications:** Indica que o sistema está em condições normais, porém de importância significativa (severidade=5). **warnings:** Mensagem de advertência (severidade=4) . Para remover a configuração, usa-se: **no logging trap**

Comandos relacionados

CPE# show logging buffer all	Exibe os logs armazenados localmente.
CPE# show logging buffer kernel	Exibe os logs relacionados ao kernel armazenados localmente.
CPE# show logging buffer pbx	Exibe os logs relacionados ao PBX armazenados localmente.
CPE# show logging buffer sip	Exibe os logs relacionados ao SIP armazenados localmente.
CPE# show logging buffer system	Exibe os logs do sistema armazenados localmente.

4.18.6. Monitor de fluxo

Para os profissionais de TI é fundamental ter conhecimento sobre a utilização dos recursos da rede, as anomalias que ocorrem e os pontos mais críticos. Um entendimento destas características permite a realização planejamentos para futuras melhorias e a obtenção de estimativas do impacto que determinadas mudanças irão causar, possibilitando assim a redução dos custos de operação através de uma melhor utilização da infra-estrutura de rede.

O software para monitoramento de fluxo presente nos equipamentos da Digistar supre estas necessidades permitindo a visualização das características de operação da rede em um dado momento e o envio constante de relatórios sobre estas características para servidores remotos (chamados de coletores).

Em relação ao SNMP que é tradicionalmente utilizado para verificar a largura de banda utilizada, a monitoração de fluxo nas interfaces traz como vantagem a completa caracterização dos padrões de tráfego, tais como: protocolo, endereços IP e portas de origem e destino, endereço MAC, entre outras informações. Assim, esta ferramenta contribui significativamente para a detecção de ataques de negação de serviço (Denial of Service – DoS) e outros eventos indesejáveis.

Um fluxo é considerado encerrado no momento em que a comunicação em rede termina, como por exemplo pelo envio de um pacote TCP com a flag FIN. Os fluxos podem ser armazenados localmente ou exportados sobre o protocolo de transporte UDP para os coletores periodicamente.

A tabela abaixo mostra os passos para configuração do monitor de fluxo.

Tabela 187: Configurações do monitor de fluxo

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE (config)# interface type number	Acessa o modo de configuração da interface.
4	CPE (config-interface)#ip flow {ingress | egress}	(Opcional) Configura a captura de fluxos na interface. Para remover esta configuração usa-se: **no ip flow ingress** **no ip flow egress**
5	CPE (config-interface)# exit	Deixa o modo de configuração da interface.
6	CPE (config)# ip flow-export destination {host-addr | hostname} udp-port {global | vrf vrf-name}	(Opcional) Configura a exportação de fluxos para um coletor. Podem ser usadas portas UDP de 1 até 65535, devendo ser observada a porta configurada no coletor. Não existe uma porta padrão. Pode ser configurada a exportação do tráfego global ou do tráfego de uma VRF. Para remover esta configuração usa-se: **no ip flow-export destination**
7	CPE (config)# ip flow-export source {dialer | ethernet | loopback} number	(Opcional) Configura a interface cujo endereço será usado como fonte para a exportação dos fluxos. Para remover esta configuração usa-se: **no ip flow-export source**
8	CPE (config)# ip flow-export version {1 | 10 | 5 | 9}	(Opcional) Os fluxos são exportados no formato Netflow (RFC 3954). Este comando configura a versão do Netflow que será usada no envio dos fluxos para o coletor. O coletor pode ser qualquer software capaz de processar o formato Netflow. Para remover esta configuração usa-se: **no ip flow-export version**
	CPE (config)# ip flow-capture mac-addresses	(Opcional) Captura endereços MAC de origem e destino. Para remover esta configuração usa-se: **no ip flow-capture mac-addresses**

	CPE (config)# ip flow-capture vlan-id	(Opcional) Captura identificadores de VLANs dos pacotes. Para remover esta configuração usa-se: **no ip flow-capture vlan-id**
	CPE (config)# ip flow-cache entries num-entries	(Opcional) Configura o número de entradas na cache, de 1024 até 524288. Para remover esta configuração usa-se: **no ip flow-cache entries**
	CPE (config)# ip flow-cache timeout {active | inactive} seconds	(Opcional) Configura os parâmetros de timeout da cache. **Parâmetros:** active é fornecido em minutos, de 1 até 60, enquanto que inactive é fornecido em segundos, de 10 até 600. Para remover esta configuração usa-se: **no ip flow-cache timeout {active | inactive}**

Comandos relacionados

CPE# show ip cache flow	Exibe as estatísticas do monitor de fluxo.

4.18.7. RMON (Remote Monitoring)

RMON (*Remote Monitoring*) permite realizar o monitoramento constante de objetos gerenciados via SNMP. Com isso é possível aumentar a flexibilidade do gerenciamento e diminuir a necessidade de acessos pelos NMS (*Netowrk Management Systems*) ao dispositivo.

O CPE implementa os seguintes grupos do RMON (consultar RMON-MIB [RFC-4502]):

- Estatísticas de Rede (RMON-MIB::etherStatsTable): coletânea de objetos referente a várias estatísticas das interfaces de redes do equipamento.
- Histórico de Redes (RMON-MIB::history): histórico das estatísticas de redes.
- Alarmes (RMON-MIB::alarm): permite a coleta constante dos valores de objetos gerenciados e a comparação em relação a limiares pré-determinados.
- Eventos (RMON-MIB::event): possibilita a geração de logs e o envio de Traps SNMP, conforme os alarmes identificados no grupo Alarmes.

Abaixo têm os passos para habilitar o RMON.

Tabela 188: Configurações do RMON

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)#snmp-server [vrf vrf-name] community community-string	Habilita o agente SNMP.
4	CPE(config)# rmon agent [vrf vrf-name]	Habilita o RMON no agente SNMP (global ou vrf). Para desabilitar o RMON num agente SNMP: **no rmon agent [vrf vrf-name]**

Uma vez habilitado, o grupo de Estatísticas e de Histórico de Rede inicializam a coleta constante dos parâmetros das interfaces de rede.

A seguir estão os comandos para criar alarmes e eventos para monitorar algum OID e gerar ações, conforme limiares desejados.

Tabela 189: Comandos para criar alarmes

Passo	Comando	Objetivo
1	CPE> enable	Entra no modo de usuário privilegiado.
2	CPE# configure terminal	Acessa o modo de configuração.
3	CPE(config)# rmon [vrf vrf-name] event {number} [log] [description string] [owner string]	Configura um evento RMON. **<u>Parâmetros</u>**: - *number*: número que identifica o enveto; - (Opcional) *log*: registra na tabela de log do RMON (RMON-MIB::logTable) quando o evento for chamado; - (Opcional) *description*: descrição do evento; - (Opcional) *owner string*: identificação do dono do evento. Observação: por padrão todos os eventos sempre que forem gerados enviam as Traps RMON-MIB::risingAlarm ou RMON-MIB::fallingAlarm, conforme o Alarme que estiverem associados; Para remover um evento: **no remon event {number}**
	Exemplo: CPE(config)# rmon event 1 log InterfaceUP Fulano CPE(config)# rmon event 2 log InterfaceDOWM Fulano	No exemplo são criados dois eventos, os quais geram uma entrada na tabela de logs do RMON e também geram uma Trap, tendo como descrições “InterfaceUP” e “ InterfaceDown” e a *string* de dono como “Fulano”.

4	CPE(config)# rmon [vrf vrf-name] alarm {number} {variable OID} {interval} {delta | absolute} rising-threshold {rs-th value} {rs-th-event-number} falling-threshold {fl-th value} {fl-th-event-number} [owner string] **Exemplo:** rmon alarm 1 ifAdminStatus.2 5 absolute rising-threshold 2 1 falling-threshold 1 2 Fulano	Configura um alarme RMON. **Parâmetros**: - *number*: número de identificação do alarme; - *variable OID*: OID do objeto SNMP a ser monitorado; - *interval*: intervalo de monitoramento; - *absolute*: testa com o limiar definido o valor atual do objeto monitorado. - *delta*: testa com o limiar definido a variação entre o último valor coletado e o valor atual do objeto monitorado. - *rising-threshold*: limiar de subida; - *rs-th-event-number*: identificação do Evento que é gerado quando o valor do objeto ultrapassa acima o limiar *rising-threshold*; - *falling-threshold:* limiar de descida*;* - *fl-th-event-number*: identificação do Evento que é gerado quando o valor do objeto ultrapassa abaixo o limiar *falling-threshold*; - (Opcional) *owner string*: identificação do dono do alarme. Para remover um evento: **no remon alarm {number}** No exemplo é criado um alarme que faz a coleta a cada 5 segundos e comparada de modo absoluto o OID ifAdminStatus.2, que contém a informação de estado administrativo da interface de rede ifIndex 2. Caso, esse objeto ultrapasse o valor de 2, é gerado o evento identificado pelo número 1, já se o objeto diminuir abaixo do valor 1, é gerado o evento 2.
5	CPE(config)#snmp-server [vrf vrf-name] community *community-string* {ro | rw}	Habilita o agente SNMP
6	CPE(config)# rmon agent [vrf vrf-name]	Habilita o RMON no agente SNMP (global ou vrf)

4.19. Configurações do SIP

As ligações IP são feitas no VoIP usando o protocolo SIP (Session Initiation Protocol, RFC3261). Este serve para negociar os parâmetros da comunicação via rede, escolhendo endereço e compactação para o envio e recepção de áudio. Depois de estabelecida a chamada, os pacotes de áudio trafegam usando o protocolo RTP (Real-time Transport Protocol, RFC3550 e RFC3551).

O protocolo SIP oferece a opção de usar um servidor SIP (Registrar/Proxy), que funciona como uma central de endereços SIP, onde cada ponto tem um nome de usuário associado ao seu endereço real. Nesse caso todas as mensagens SIP para outros pontos registrados no servidor Registrar/Proxy serão encaminhadas para o servidor, que através de seu banco de dados de usuários registrados irá encaminhá-las para o endereço correto. Isso é usado pelas operadoras VoIP.

Quando uma chamada é negociada, o protocolo de sinalização usado (SIP) precisa passar para o outro ponto de comunicação o endereço para onde deve ser enviado o áudio. Esse endereço precisa ser acessível a partir do outro ponto de comunicação, caso contrário a conexão não terá áudio. Se a interface do CPE estiver conectada à Internet através de um NAPT, ou seja, tiver um endereço IP de uma rede interna não-roteável, o STUN deverá ser habilitado para que as ligações VoIP tenham áudio.

Tabela 190: Configurações SIP

Passo	Comando	Objetivo
	CPE> enable	Entra no modo de usuário privilegiado.
	CPE# configure terminal	Acessa o modo de configuração.
	CPE(config)# sip	Entra na configuração do SIP
	CPE(config-sip)# no vsp {VSP} CPE(config-sip)# vsp {VSP}	Entra no nível de configuração do servidor SIP, “(config-sip-vspX)”. O parâmetro vsp é o número do servidor, que pode ser ‘1’ à ‘5’. O comando precedido de ‘no’ desabilita a operadora e não troca de nível.
	CPE(config-sip-vspX)# no only-proxy CPE(config-sip-vspX)# only-proxy	Configura a operadora para usar “somente proxy”. O comando precedido de ‘no’ desabilita essa configuração

	CPE(config-sip-vspX)# no server CPE(config-sip-vspX)# server {FQDN} {VRF}	Configura o endereço do servidor da operadora. O parâmetro fqdn é o endereço FQDN do servidor. O item VRF é opcional, quando é necessário associar alguma VRF ao Cliente Registrar. O comando precedido de 'no' desabilita essa configuração.
	CPE(config-sip-vspX)# no expire-time CPE(config-sip-vspX)# expire-time {TIME}	Configura o tempo de expire para a operadora. O comando precedido de 'no' desabilita essa configuração
	CPE(config-sip-vspX)# no sip-port CPE(config-sip-vspX)# sip-port {PORT}	Configura a porta SIP para a operadora. O comando precedido de 'no' desabilita essa configuração.
	CPE(config-sip-vspX)# protocol {PROT}	Configura o protocolo de transporte a ser utilizado pela operadora Registar. O parâmetro prot define o protocolo e pode ter os seguintes valores: tcp: Usa TCP como protocolo de transporte udp: Usa UDP como protocolo de transporte
	CPE(config-sip-vspX)# dtmf {SRC}	Configura a forma do tratamento dos sinais DTMF. O parâmetro src define o modo e pode ter esses valores: Inband:Usa DTMF dentro da banda outband: Usa DTMF fora da banda, de acordo com a RFC2833.
	CPE(config-sip-vspX)# cid from uri CPE(config-sip-vspX)# cid from display-name CPE(config-sip-vspX)# cid contact	Configura o campo que a servidor SIP irá utilizar como identificador de chamadas.
	CPE(config-sip-vspX)# ddr to uri CPE(config-sip-vspX)# ddr to display-name CPE(config-sip-vspX)# ddr contact	Configura o campo que a Servidor SIP irá utilizar como DDR.
	CPE(config-sip-vspx)# no only-proxy CPE(config-sip-vspx)# only-proxy	Configura a operadora para usar "somente proxy". O comando precedido de 'no' desabilita essa configuração
	CPE(config-sip-vspx)# no proxy-server CPE(config-sip-vspx)# proxy-server {FQDN}	Configura um endereço FQDN como servidor proxy para a operadora. O comando precedido por 'no' desabilita essa configuração.
	CPE(config-sip-vspx)# codec {CODEC}	Configura o codec preferencial a ser utilizado pelo SIP. Os valores do parâmetro codec são: g729 Utiliza o codec G.729 como codec preferencial g711a Utiliza o codec G.711-A como codec preferencial g711u Utiliza o codec G.711-U como codec preferencial

	CPE(config-sip-vspx)# codec fax {CODEC}	Configura o codec a ser utilizado nas transmissões de fax. O parâmetro codec pode ter os seguintes valores: g711a: Utiliza o codec G.711-A como codec de fax g711u Utiliza o codec G.711-U como codec de fax t38:Utiliza o codec T.38 como codec de fax
	CPE(config-sip-vspx)#restricted-id teste	Configura com números ou palavras o que deve ser enviado no campo “restrict-id”.
	CPE(config-sip- vspx)# no vad CPE(config-sip-vspx)# vad	Habilita a detecção de presença de voz no sip. O comando precedido de ‘no’ desabilita essa configuração.
	CPE(config-sip-vspx)# dtmf {SRC}	Configura a forma do tratamento dos sinais DTMF. O parâmetro src define o modo e pode ter esses valores: inband: Usa DTMF dentro da banda outband:Usa DTMF fora da banda, de acordo com a RFC2833.
	CPE(config-sip-vspx)# ddr to uri CPE(config-sip-vspx)# ddr to display-name CPE(config-sip-vspx)# ddr contact	Configura o campo que a operadora Registar irá utilizar como DDR.
	CPE(config-sip-vspx)# no prack CPE(config-sip-vspx)# prack	Habilita o uso de PRACK pela operadora Registar. O comando precedido de ‘no’ desabilita essa configuração
	CPE(config-sip-vsp1)#signalling {OPÇÃO} OPÇÃO: 180 Sends 180 response 180-sdp Sends SDP info on 180 response 183-sdp Sends SDP info on 183 response	Sinalização configurável para respostas 180(RINGING)/180+SDP/183(SESSION IN PROGRESS) em ligações de entrada atendidas pelo Gateway/PABX.
	CPE(config-sip-vspx)# no compact-headers CPE(config-sip-vspx)# compact-headers	Habilita o uso de cabeçalhos compactos pela operadora Registar. O comando precedido de ‘no’ desabilita essa configuração.
	CPE(config-sip)#account {NUM} ou range CPE(config-sip)#no account {NUM}	Entra no nível de configuração das contas SIP, NUM varia de 1 ate 1000 ou Range. O comando com ‘no’ desabilita a conta.

	CPE(config-sip)#account range {NUM , - } Ex: account range 1-100 CPE(config-sip-acc-1-100)#set-range {opções} {valor} Opções: Auth-user Contact Display name Restrict-id User Ex. CPE(config-sip-acc-1-100)#set-range user 200	Configura contas individualmente ou intervalos de contas Sip . Pode ser configurado um range de usuários , contact, display name a única observação é que não pode ser configurada a senha no range de contas. O campo valor define o valor da primeira conta do range, os próximos valores serão incrementados a cada conta aplicada. O exemplo mostra que foram criadas 100 contas onde os usuários configurados foram de 200 á 299.
	CPE(config-sip-acc-N)# no user CPE(config-sip-acc-N)# user {USER} pass {PASSW}	Configura um usuário e senha para a conta 1. O comando precedido de 'no' desabilita essa configuração.
	CPE(config-sip-acc-N)# no auth-user CPE(config-sip-acc-N)# auth-user {USER}	Configura um usuário de autenticação para a conta 1. O comando precedido de 'no' desabilita essa configuração
	CPE(config-sip-acc-N)# no display-name CPE (config-sip-acc-N)# display-name {NAME}	Configura o campo "display name" para a conta 1. O comando precedido de 'no' desabilta essa configuração.
	CPE(config-sip-acc-N)# no contact {NAME} CPE(config-sip-acc-N)# contact {NAME}	Configura o campo "contact" para a conta 1. O comando precedido de 'no' desabilta essa configuração.
	CPE(config-sip-acc-N)# server {1-5}	Associa um dos servidores (1-5) configurados na conta N
	CPE(config-sip-acc-N)# no allow-simult CPE(config-sip-acc-N)# allow-simult	Ativa que entre ligações simultâneas na conta configurada. O comando precedido de 'no' desabilta essa configuração.
	CPE(config-sip)# rtp port-range {PORT1} {PORT2} dscp {DSCP}	Configura o intervalo de portas para o RTP. O parâmetro port1 é a porta inicial do RTP e o parâmetro port2 é a porta final do range. O parâmetro dscp é o valor DSCP associado aos pacotes RTP. Esse parâmetro pode ser: best-effort: Usa o método "best effort" para o DSCP ip-precedence {VAL}: Usa o método "ip precedence". O parâmetro val varia de '1' até '7'. af-class {VAL} {TYPE}: Usa o método "af class". O parâmetro val varia de '1' até '4' e o parâmetro type pode ser "low", "medium" ou "high". ef-class: Usa o método "ef class" para o DSCP.

	CPE(config-sip)# integrated-sip	Configuração dos pontos remotos
	CPE(config-sip-is)#sip-int {1-64} {NAME} {FQDN} {PORT} {VRF}	Configura o ponto remoto de 1-64 , programando o nome, fqdn do destino, porta e a VRF é opcional.
	CPE(config-sip)# no shutdown CPE(config-sip)# shutdown	Desabilita o serviço para poder configurar. Caso tente configurar o serviço com ele em execução, uma mensagem será mostrada indicando que o serviço deverá ser parado para poder configurar. O comando precedido de 'no' reinicia o serviço. Caso alguma configuração tenha sido efetuada e o serviço permanecer desabilitado, ao sair do nível do SIP o serviço será iniciado automaticamente.

4.20. Configurações TDM

Tabela 191: Configurações TDM

Passo	Comando	Objetivo
	CPE> enable	Entra no modo de usuário privilegiado.
	CPE# configure terminal	Acessa o modo de configuração.
	CPE(config)#pbx	Entra no nível de configuração da parte referente ao PABX.
	CPE(config-pbx)#digital-line	Entra no modo de configuração do tronco digital.
	CPE(config-pbx-dline1)#clock-mode {master|slave}	Configura o modo do clock do tronco digital, se master ou slave.
	CPE(config-pbx-dline1)#trunk-mode {r2|isdn}	Configura o modo do tronco digital, de R2 ou ISDN.
	CPE(config-pbx-dline1)#r2-standard {std}	Configura a região do R2 conforme as opções abaixo: arg Padrão Argentino bra Padrão Brasileiro chl Padrão Chileno mex Padrão Mexicano
	CPE(config-pbx-dline1)#channels {NUM}	Nesta configuração o parâmetro "NUM" é o número de canais que devem ser ativados.
	CPE(config-pbx-dline1)# digits {DIG}	Nesta configuração o DIG é o número de dígitos DDR que devem ser enviados.
	CPE(config-pbx-dline1)# enable ccb CPE(config-pbx-dline1)# no enable ccb	Nesta configuração ativamos o BCC e precedido do "no" desativamos.
	CPE(config-pbx-dline1)# enable idc CPE(config-pbx-dline1)# no enable idc	Nesta configuração ativamos o IDC e precedido do "no" desativamos.
	CPE(config-pbx-dline1)# no crc-4 CPE(config-pbx-dline1)# crc-4 CPE(config-pbx-dline1)# crc-4 automatic	Configura o modo do CRC-4, habilitado, desabilitado ou automático.
	CPE(config-pbx-dline1)#line-signaling incoming {parametro1} outgoing {parametro2}	Sinalização de Linha. O {parametro1} e {parametro2} podem ser configurados como "digital" ou "analog"

	CPE(config-pbx-dline1)#register-signaling incoming {parametro1} outgoing {parametro2}	Sinalização de Registradores. O {parametro1} e {parametro2} podem ser configurados como “mfc” ou “dtmf”.
	CPE(config-pbx-dline1)#occupation {decreasing|increasing}	O parametro é configurado com “decreasing“ ou “increasing” dependendo de que forma será a ocupação dos troncos incrementando ou decrementando.
	CPE(config-pbx-dline1)#digit-timeout {NUM}	Nesta configuração o parâmetro de NUM é entre {1-10} tempo que pode ser programado entre dígitos.
	CPE(config-pbx-dline1)#co ld-code {DDD} Exemplo: CPE(config-pbx-dline1)#co ld-code 51	Nesta configuração é setado o DDD da região. Está opção deverá ser programada quando o CPE estiver no modo Slave
	CPE(config-pbx-dline1)#co number {NUM} Exemplo: CPE(config-pbx-dline1)#co number 33749200	Configurar o número chave da central pública. Está opção deverá ser programada quando o CPE estiver no modo Slave
	CPE(config-pbx-dline1)# dialling-mode {overlap|enblock}	Configura o modo de discagem do ISDN master: overlap ou enblock.
	CPE(config-pbx-dline1)# no forward presentation-indicator CPE(config-pbx-dline1)# forward presentation-indicator	Configura o presentation-indicator, o comando precedido de ‘no’ desabilita a configuração.
	CPE(config-pbx-dline1)# mfc-absent-time <1-30>	Configura o tempo de MFC ausente.
	CPE(config-pbx-dline1)# no r2-register fim CPE(config-pbx-dline1)# no r2-register idc CPE(config-pbx-dline1)# no r2-register ani CPE(config-pbx-dline1)# r2-register fim CPE(config-pbx-dline1)# r2-register idc CPE(config-pbx-dline1)# r2-register ani	Configura os registradores FIM, IDC e ANI do R2 quando configurado na região “argentina”. O comando precedido de ‘no’ desabilita o registrador
	CPE(config-pbx)#dial-analisis dial {DIAL} digits {DIG} [collect]	Configura as regras de análise de dígito para E1 em modo Master. DIAL: A regra de discagem DIG: Número de dígitos Collect: Parâmetro opcional que define que a regra é a cobrar.
	CPE(config-pbx)#channels group ? Opções: E1 VOIP Exemplo: 30 canais no primeiro grupo. CPE(config-pbx)#channels group e1 30 0 0 0 0 0 0 0 0 0	Neste nível é configurado quantidade de canais por grupo.
	CPE(config-pbx)#group ? Opções: E1 Voip Exemplo: CPE(config-pbx)#group e1 slot {0-9} ? Description Type	Neste nível é configurado o tipo de cada grupo(slot).

	Exemplo: CPE(config-pbx)#group e1 slot 0 type {opção} Opção: Bidirecional Incoming Outgoing	
	CPE (config-pbx)# redirection input {E1| Integrated-sip | voip-operator} groups {0-9} from {CID} to {NUMBER1} output {E1| Integrated-sip | voip-operator | Disa} groups {0-9} from {CID} to {NUMBER2} Exemplo: CPE (config-pbx)# redirection input E1 groups 0 from * to 206 output Integrated-sip 2 groups 0 from {From} to 2{To:1}	Os parâmetros são: CID: comando onde se configura o IDC que deve ser substituído, caso não precise ser substituído colocar "*".Pode ser configurado com a Conta ou ponto remoto do SIP, caso a configuração seja do Sip Integrado ou Op.Voip. Groups: deve ser configurado para designar por quais canais deverão entrar e sair as ligações. to NUMBER1 e from NUMBER2 : Estes campos possuem diversos significados dependendo do tipo de entrada. Exemplo: Se a entrada for do Tipo E1 (slave) conectado a uma operadora. From = CID seria um DDD+ 8 ou 9 dígitos ou *. To = NUMBER1 seria um DDR de 3 ou 4 dígitos.. A interface de saída no caso de um Sip Integrado From = CID seria * se for usado o mesmo IDC de entrada. To = NUMBER2 seria o número do ramal do ponto remoto. Opção Disa: pode ser configurado na interface de saída, esta opção direciona ligações para uma mensagem gravada. Durante esta mensagem o usuário pode discar até 20 dígitos. Depois da discagem é capturado estes dígitos e aplicado novamente nas regras. OBS: Ao programar uma entrada com a opção E1 ou Voip-operator a opção de saída libera opções diferentes. Exemplo: Se input for igual E1 o output libera Integrated-sip | voip-operator | Disa.

	CPE(config-pbx)#voip-gain {OPÇÃO} percent {%} OPÇÃO: rx Reception gain tx Transmission gain %: 0 0% gain 25 25% gain 50 50% gain 75 75% gain 100 100% gain 125 125% gain 150 150% gain 175 175% gain	Ajuste do ganho no audio entre ligações.

5. Anexo I - Status enviado do SIP para o ISDN no encerramento de ligações.

SIP		ISDN	
Status	**Motivo**	**Return**	**Status**
case 400	// Bad request	PRI_CAUSE_INTERWORKING	127
case 401	// Unauthorized	PRI_CAUSE_BEARERCAPABILITY_NOTAUTH	57
case 402	// Payment required	PRI_CAUSE_CALL_REJECTED	21
case 403	// Forbidden	PRI_CAUSE_BEARERCAPABILITY_NOTAUTH	57
case 404	// Not found	PRI_CAUSE_UNALLOCATED	1
case 405	// Method not allowed	PRI_CAUSE_INTERWORKING	127
case 406	// Not acceptable	PRI_CAUSE_INTERWORKING	127
case 407	// Proxy authentication required	PRI_CAUSE_CALL_REJECTED	21
case 408	// Request timeout	PRI_CAUSE_RECOVERY_ON_TIMER_EXPIRE	102
case 409	// Conflict	PRI_CAUSE_NORMAL_TEMPORARY_FAILURE	41
case 410	// Gone	PRI_CAUSE_UNALLOCATED	1
case 411	// Length required	PRI_CAUSE_INTERWORKING	127
case 413	// Request entity too long	PRI_CAUSE_INTERWORKING	127
case 414	// Request URI (URL) too long	PRI_CAUSE_INTERWORKING	127
case 415	// Unsupported media type	PRI_CAUSE_SERVICE_OR_OPTION_NOT_AVAILABLE	79
case 420	// Bad extension	PRI_CAUSE_INTERWORKING	127
case 480	// Temporarily unavailable	PRI_CAUSE_NO_USER_RESPONSE	18
case 481	// Call leg does not exist	PRI_CAUSE_INTERWORKING	127
case 482	// Loop detected	PRI_CAUSE_INTERWORKING	127
case 483	// Too many hops	PRI_CAUSE_INTERWORKING	127
case 484	// Address incomplete	PRI_CAUSE_INVALID_NUMBER_FORMAT	28
case 485	// Address ambiguous	PRI_CAUSE_UNALLOCATED	1
case 486	// Busy here	PRI_CAUSE_USER_BUSY	17
case 487	// Request canceled	PRI_CAUSE_INTERWORKING	127
case 488	// Not acceptable here	PRI_CAUSE_INTERWORKING	127
case 500	// Internal server error	PRI_CAUSE_NORMAL_TEMPORARY_FAILURE	41
case 501	// Not implemented	PRI_CAUSE_SERVICE_OR_OPTION_NOT_AVAILABLE	79
case 502	// Bad gateway	PRI_CAUSE_NETWORK_OUT_OF_ORDER	38
case 503	// Service unavailable	PRI_CAUSE_SERVICEOROPTION_NOTAVAIL	63
case 504	// Gateway timeout	PRI_CAUSE_RECOVERY_ON_TIMER_EXPIRE	102
case 505	// Version not implemented	PRI_CAUSE_INTERWORKING	127
case 580	// Precondition failed	PRI_CAUSE_BEARERCAPABILITY_NOTAVAIL	58
case 600	// Busy everywhere	PRI_CAUSE_USER_BUSY	17
case 603	// Decline	PRI_CAUSE_CALL_REJECTED	21
case 604	// Does not exist anywhere	PRI_CAUSE_UNALLOCATED	1
case 606	// Not acceptable	PRI_CAUSE_BEARERCAPABILITY_NOTAVAIL	58